TASK ORDER

GST0012AJ0127

USCENTCOM C4 Enterprise Support

IN SUPPORT OF:

United States Central Command

Issued to:

SAIC
One North Dale Mabry HWY
Suite 400
Tampa, FL 33609

issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street NW
Suite 3100
Washington DC 20405
August 24, 2012

FEDSIM Project Number 11041DEM

NOTE: The Section numbers in this Task Order (TO) correspond to the Section numbers in the Alliant Contract. Only those Sections listed from the Alliant Basic apply to this Task Order.

B.1 GENERAL

The work shall be performed in accordance with all Sections of this TO and the Contractor's Basic Contract, under which the resulting TO will be placed. An acronym listing to support this Task Order Request (TOR) is included in Section J, Attachment J.

B.5 CONTRACT ACCESS FEE

The General Services Administration's (GSA) operating costs associated with the management and administration of this contract are recovered through a Contract Access Fee (CAF). The amount of the CAF is ¾ % (i.e., (.0075)) of the total price/cost of Contractor performance. Each TO issued under this contract shall have a separate Contract Line Item Number (CLIN) to cover this access fee, and this CAF shall be obligated at TO award. The following access fee applies to TO issued under this contract.

GSA-Issued Task Orders:
Orders in excess of $13.3 million are capped at $100,000 per order year.

B.6 ORDER TYPES

The Contractor shall perform the effort required by this TO on a Cost-Plus-Award-Fee (CPAF) basis for CLINs 0001, 1001, 2001, 3001, 4001, and 0002, 1002, 2002, 3002, 4002 and on a Not-to-Exceed (NTE) basis for CLINs, 0003, 1003, 2003, 3003, 4003, 0004, 1004, 2004, 3004, 4004, 0005, 1005, 2005, 3005, 4005, 0006, 1006, 2006, 3006, and 4006.

B.7 ORDER PRICING (ALL ORDER TYPES)

The following abbreviations are used in this price schedule:

CPAF	Cost-Plus-Award-Fee
CLIN	Contract Line Item Number
ODC	Other Direct Cost
NTE	Not-to-Exceed

B.7.1 SERVICES AND PRICES/COSTS

B.7.1.1 BASE PERIOD:

MANDATORY LABOR CLINs

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
0001A	Labor (Tasks 1–7 except Subtask 6.4 (C.5.6.4)	(b) (4)	(b) (4)	$41,768,864

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
0001B	Labor (Task 8)	(b) (4)	(b) (4)	$10,603,636

OPTIONAL LABOR CLIN

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
0002	Labor (Subtask 6.4 (C.5.6.4))	(b) (4)	(b) (4)	$425,923

TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description	Estimated Cost	Fixed Fee	Total Ceiling Price
0003	Long Distance Travel Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$ 900,000
0004	Tools Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$8,326,000.00
0005	ODCs Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$3,000,000
0006	Contract Access Fee	N/A	N/A	$100,000

TOTAL CEILING BASE PERIOD CLINs: **$65,124,423**

B.7.1.2 FIRST OPTION PERIOD:

MANDATORY LABOR CLINs

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
1001A	Labor (Tasks 1–7)	(b) (4)	(b) (4)	$65,657,189

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
1001B	Labor (Task 8)	(b) (4)	(b) (4)	$10,921,745

OPTIONAL LABOR CLIN (deleted Mod PS06)

TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description	Estimated Cost	Fixed Fee	Total Ceiling Price
1003	Long Distance Travel Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$1,000,000
1004	Tools Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$6,325,000
1014	Procurement Tools	(b) (4)	(b) (4)	$2,531,087
1005	ODCs Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$3,100,000
1006	Contract Access Fee	N/A	N/A	$100,000

TOTAL CEILING FIRST OPTION PERIOD CLINs: **$89,635,021**

B.7.1.3 SECOND OPTION PERIOD:

MANDATORY LABOR CLINs

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
2001A	Labor (Tasks 1–7)	(b) (4)	(b) (4)	$65,629,119

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
2001B	Labor (Task 8)	(b) (4)	(b) (4)	$11,239,855

OPTIONAL LABOR CLIN (deleted Mod PS06)

TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description	Estimated Cost	Fixed Fee	Total Ceiling Price
2003	Long Distance Travel Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$1,100,000
2004	Tools Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$7,094,141
2014	Procurment Tools	(b) (4)	(b) (4)	$3,623,772
2005	ODCs Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$3,100,000
2006	Contract Access Fee	N/A	N/A	$100,000

TOTAL CEILING SECOND OPTION PERIOD CLINs: **$91,886,887**

B.7.1.4 THIRD OPTION PERIOD:

MANDATORY LABOR CLINs

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
3001A	Labor (Tasks 1–7)	(b) (4)	(b) (4)	$66,329,089

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
3001B	Labor (Task 8)	(b) (4)	(b) (4)	$11,664,000

OPTIONAL LABOR CLIN (deleted Mod PS06)

TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description	Estimated Cost	Fixed Fee	Total Ceiling Price
3003	Long Distance Travel Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$1,200,000
3004	Tools Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$9,900,000
3005	ODCs Including DCMA/ Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$3,300,000
3006	Contract Access Fee	N/A	N/A	$100,000

TOTAL CEILING THIRD OPTION PERIOD CLINs: **$92,493,089**

B.7.1.5 FOURTH OPTION PERIOD:

MANDATORY LABOR CLINs

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
4001A	Labor (Tasks 1–7)	(b) (4)	(b) (4)	$67,201,200

CLIN	Description	Estimated Cost	Award Fee	Total Estimated Cost Plus Award Fee
4001B	Labor (Task 8)	(b) (4)	(b) (4)	$11,982,109

OPTIONAL LABOR CLIN (deleted Mod PS06)

TRAVEL, TOOLS, and ODCs CLINs

CLIN	Description	Estimated Cost	Fixed Fee	Total Ceiling Price
4003	Long Distance Travel Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$1,300,000
4004	Tools Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$10,200,000
4005	ODCs Including DCMA Approved Provisional Indirect Handling Rate	(b) (4)	(b) (4)	$3,400,000
4006	Contract Access Fee	N/A	N/A	$100,000

TOTAL CEILING FOURTH OPTION PERIOD CLINs: **$ 94,183,309**

GRAND TOTAL CEILING ALL CLINs: **$433,322,729**

The Government will adjust the award fee pool to be proportional to the level of effort/ cost incurred during the award fee evaluation period for SUBCLINs 0001b, 1001b, 2001b, 3001b and 4001b. **In addition, the Government reserves the right to adjust the fixed fee pool for SUBCLINs 0004, 0005, 1004, 1005, 2004, 2005, 3004, 3005, 4004, 4005, to remain proportional to the costs of Tools and ODCs expended during the reporting period.**

B.7.6 INDIRECT/MATERIAL HANDLING RATE

Travel, Tools, and ODC costs incurred may be burdened with the Contractor's approved DCMA Provisional indirect/material handling rate.

B.7.6.1 DIRECT AND INDIRECT RATES

B.7.6.1.1 DIRECT LABOR RATES

Labor categories proposed shall be mapped to existing Alliant labor categories with the exception of any other proposed unique labor categories that are not currently on the Alliant GWAC.

B.7.6.1.2 INDIRECT LABOR RATES

All indirect rates proposed and billed under this TO shall be commensurate with the then current DCAA approved forward pricing rate agreement. Indirect rates include, but may not be limited to, indirect material handling rates, overhead rates, and general and administrative rates.

B.8 TRAVEL PRICING

Long distance travel is defined as travel over 50 miles. Local travel will not be reimbursed.

B.12 INCREMENTAL FUNDING

B.12.1 INCREMENTAL FUNDING LIMITATION OF GOVERNMENT'S OBLIGATION

Incremental funding for CLINs 0001A through 2006 is currently allotted and available for payment by the Government. Additional incremental funding for these CLINs will be allotted and available for payment by the Government as the funds become available. The estimated period of performance covered by the allotments for the mandatory CLINs is from award through **June 6, 2015** unless otherwise noted in Section B.7.1. The TO will be modified to add funds incrementally up to the maximum of $433,322,729 over the performance period of this TO. These allotments constitute the estimated cost for the purpose of Federal Acquisition Regulation (FAR) Clause 52.232-22, Limitation of Funds, which applies to this TO on a CLIN-by-CLIN basis.

Incremental Funding Chart for CPAF has been relocated to Section J Attachment S

B.13.2 AWARD FEE CALCULATION TABLE

Award Fee					
Year	**Period**	**Months Covered**	**Available Award Fee Pool**	**Earned Fee**	**Unearned Fee**
Base Year	1	Sep 7, 2012 – Mar 6, 2013	(b) (4)	(b) (4)	(b) (4)
Base Year	2	Mar 7 - Sep 6, 2013	(b) (4)	(b) (4)	(b) (4)
Option Year 1	3	Sep 7, 2013 – Mar 6, 2014	(b) (4)	(b) (4)	(b) (4)
Option Year 1	4	Mar 7 - Sep 6, 2014	(b) (4)	(b) (4)	(b) (4)
Option Year 2	5	Sep 7, 2014 – Mar 6, 2015	(b) (4)	(b) (4)	(b) (4)
Option Year 2	6	Mar 7 - Sep 6, 2015	(b) (4)		
Option Year 3	7	Sep 7, 2015 – Mar 6, 2016	**TBD**		
Option Year 3	8	Mar 7 - Sep 6, 2016	**TBD**		
Option Year 4	9	Sep 7, 2016 – Mar 6, 2017	**TBD**		
Option Year 4	10	Mar 7 - Sep 6, 2017	**TBD**		

C.1 BACKGROUND

The United States Central Command (USCENTCOM) Command, Control, Communications, and Computer Systems (C4) operations must reside as one enterprise program, supporting planning, program and project management, integration, operation, and maintenance of the joint global theater-level communications and computer networks for the USCENTCOM Area of Responsibility (AOR). Under this effort, the Contractor provides a full range of Information Technology (IT) services.

C.1.1 PURPOSE

The USCENTCOM C4 goal is to achieve full interoperability of the C4 systems on and off the battlefield among the United States (U.S.), Allied, and Coalition forces and to gain efficiencies of scale to establish a world class network operation.

C.1.2 AGENCY MISSION

USCENTCOM, working with national and international partners, promotes development and cooperation among nations, responds to crises, and deters or defeats state and transnational aggression in order to establish regional security and stability.

USCENTCOM is one of nine Department of Defense (DoD) unified commands. The Command has a foundation that includes global communications capabilities and programs that address information and systems management, information operations, assurance, and interoperability. CCJ6 will effectively and efficiently enable information sharing through a Joint and Combined C4 Network-Centric Environment that is flexible, redundant, reliable, and secure.

C.2 SCOPE

The effort will support all USCENTCOM C4 Directorate (CCJ6) IT programs and assets at the Headquarters (HQ), Forward Headquarters (CFH), and Security Cooperation Organizations (SCOs). The Contractor shall provide IT support services for the C4 systems that support HQ USCENTCOM in Tampa, Florida and throughout their AOR. The scope of this acquisition is to provide a full range of IT services to include: cyber defense, network operations and maintenance, IT training, IT planning, system integration, technical testing and evaluation, analysis and guidance, software customization, systems administration, hardware and software purchase, hardware repair and enhancements, helpdesk services, software configuration, architecture and infrastructure management, system management, and all deliverables related to these services.

C.3 CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

See Attachments N and P for information on the current IT network environment.

C.4 OBJECTIVE

The objective of this TO is to assist USCENTCOM in their goal to achieve full interoperability of the C4 systems in HQ USCENTCOM and AOR among the U.S., Allied, and Coalition forces and to gain efficiencies of scale to establish a world class network operation.

C.5 TASKS

C.5.1 TASK AREA 1 – PROVIDE PROGRAM MANAGEMENT

The Contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by Contractor personnel, including subcontractors, to satisfy the requirements identified in this Performance Work Statement (PWS). The Contractor shall identify a Program Manager by name who shall provide management, direction, administration, quality assurance, and leadership of the execution of this TO.

C.5.1.1 COORDINATE A PROJECT KICK-OFF MEETING

The Contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include Key Contractor Personnel, representatives from the directorates, other relevant Government personnel, and the Federal Systems Integration and Management Center (FEDSIM) Contracting Officer's Representative (COR). The Contractor shall provide the following at the Kick-Off meeting:

- Updated Transition-In Plan (Government Comments shall be incorporated into the Final Transition-In Plan)
- Project Management Plan
- Final Quality Control Plan (QCP)

C.5.1.2 PREPARE A MONTHLY STATUS REPORT (MSR)

The Contractor Program Manager shall develop and provide an MSR using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the USCENTCOM Technical Point of Contact (TPOC) and the COR (Section J, Attachment Q). The MSR shall include the following:

- Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
- Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
- Personnel gains, losses, and status (security clearance, etc.).
- Government actions required.
- Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
- Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for reporting period).
- Accumulated invoiced cost for each CLIN up to the previous month.

- Projected cost of each CLIN for the current month.

C.5.1.3 CONVENE TECHNICAL STATUS MEETINGS

The Contractor Program Manager shall convene a monthly TO Activity and Status Meeting with the TPOC, COR, and other vital Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

C.5.1.4 PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The Contractor shall document all support requirements in a PMP. The PMP shall:

- Describe the proposed management approach.
- Contain detailed Standard Operating Procedures (SOPs) for all tasks.
- Include milestones, tasks, and subtasks required in this TO.
- Provide for an overall Level 3 Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.
- Include the Contractor's Quality Control Plan (QCP)

The Contractor shall provide the Government with a draft PMP on which the Government will make comments. The final PMP shall incorporate the Government's comments.

The PMP is an evolutionary document that shall be updated annually at a minimum. The Contractor shall work from the latest Government-approved version of the PMP.

C.5.1.5 DEVELOP A DISASTER RECOVERY PLAN

The Contractor shall develop a Disaster Recovery Plan for Continuity of Operations (COOP) for Government approval. The Contractor shall designate a list of Contractor personnel as a Disaster Recovery Team and provide this list and any associated recall information. In the event of a disaster, the Disaster Recovery Team shall assess damage to systems/networks within the scope of this TO and recommend Courses of Action (COAs) to USCENTCOM to mitigate damage and expedite system/network restoral. The Disaster Recovery Team shall implement the COA selected by USCENTCOM to restore systems and networks to operational status. In the event of a natural disaster, the Contractor shall utilize a pre-designated Disaster Recovery Team to provide on-site operations until the USCENTCOM Commander orders an evacuation.

C.5.1.6 PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location.

C.5.1.7 UPDATE QUALITY CONTROL PLAN (QCP)

The Contractor shall update the QCP submitted with their proposal and provide a final QCP as required in Section F. The Contractor shall periodically update the QCP, as required in Section F, as changes in program processes are identified.

C.5.1.8 STAFFING MATRIX

The Contractor shall develop and update a staffing matrix to show arriving, departing, and transfers of Contractor personnel on the TO. The matrix shall include, at a minimum: task numbers, job descriptions, names, arrival and departure dates, and company names.

C.5.1.9 TRANSITION-IN

The Contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. All transition activities shall be completed 50 calendar days after the start date of the order. The Contractor shall deliver an updated draft of their proposed Transition-In Plan within five workdays of award.

C.5.1.10 TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The Contractor shall provide and implement a Transition-Out Plan NLT 90 calendar days prior to expiration of the TO. The Contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

- Project management processes
- Points of contact
- Location of technical and project management documentation
- Status of ongoing technical initiatives
- Appropriate Contractor-to-contractor coordination to ensure a seamless transition
- Transition of Key Personnel
- Schedules and milestones
- Actions required of the Government

The Contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings.

C.5.2 TASK AREA 2 - C4 SYSTEMS SUPPORT

The Contractor shall provide the following support for all of the tasks/subtasks under this Task Area where appropriate:

1. Provide technical expertise to the USCENTCOM Very Important Person (VIP) team.
2. Provide on-site support in accordance with (IAW) HQ USCENTCOM policies, regulations, regulations guidelines and Memorandum of Agreements (MOAs).

3. Ensure all scheduled and unscheduled service outages are identified and coordinated IAW USCENTCOM policies, regulations, and guidelines. Scheduled outages shall be performed at a time that cause the least mission impact and inconvenience to users.
4. Maintain 100% accountability of all assets within the scope of this task area. Track and provide budgeting, forecasting, and consumption rate information in order to best utilize and manage spare equipment and ensure all necessary repair parts are available to quickly return assets to operational status.
5. Perform, schedule, and document PMIs on the systems, devices, and associated hardware within the scope of this task IAW manufacturer's manuals and/or vendor best practice recommendations. Maintain PMI completion documents on file for review by USCENTCOM upon request. The Contractor shall create and maintain a schedule to perform preventive maintenance IAW the equipment manufacturer's manuals and USCENTCOM direction. PMIs shall be annotated in the schedule. Provide preventive, remedial, and corrective maintenance to ensure all on-line and spare equipment, to include spare equipment strings, is in proper and full operating condition as described by the equipment manufacturer and applicable DISA circulars without degradation of service. All equipment, regardless of whether or not it is providing service at any particular time, shall be maintained in fully operational condition.
6. The contractor shall investigate, troubleshoot, and repair information exchange issues between the USCENTCOM information technology enterprise and those of other organizations who support USCENTCOM missions; to include Department of State and foreign military organizations.
7. Monitor USCENTCOM's IT Service Desk queues for applicable trouble tickets, change requests, and work orders to take the appropriate action to expedite processing and resolve customer-related incidents, changes, and problems.
8. Maintain 100% accountability of all communications security (COMSEC) -related items IAW National Security Agency (NSA)/DoD/USCENTCOM COMSEC policies, guidelines and procedures.
9. Recommend a prioritized service restoration list for returning systems and services to operation in the event of a catastrophic failure, to restore station lines, systems, devices, cabling, and for returning systems and services to operation in the event of a catastrophic failure. The identity and location of circuits may vary over the life of the TO and shall be provided by USCENTCOM. The list shall be prioritized by each network and system/device operated and maintained by the contractor. The list shall also include information on customer types, priorities, locations, and any spare parts/equipment requirements. The list shall be updated as changes occur either to the system architecture or to the supported customers. The list shall be published on a quarterly basis.
10. Coordinate with Configuration Management to ensure that any new or updated records for configuration items within the scope of this task area are entered in the CMDB IAW USCENTCOM standards.
11. Update/generate documentation and artifacts required to support inspections for any network/system within the scope of this task.
12. Publish periodic reports (monthly, quarterly, and/or annually). These reports shall include trend analysis of common problems and system performance, change requests,

average device and service uptime, service outage durations and frequencies, trouble ticket status updates, analyses of training effectiveness, statistics on courses conducted and other parameters identified as necessary to best report on the state of the USCENTCOM enterprise.

13. Review, edit, and maintain diagrams within 30 calendar days after TO award IAW USCENTCOM, regulations, policies and standards. Maintain newly developed and existing diagrams and synchronize any modifications IAW DIACAP standards. Updates to these physical and logical diagrams of systems, networks, infrastructure and storage shall be completed within 24 hours after any changes have been implemented. Validated versions of these physical diagrams shall be published in the standardized format specified by agreed to by the USCENTCOM and the contractor at least on a monthly basis.
14. Maintain a continuity folder of documentation pertaining to all systems and technologies that are relevant to this task area in order to facilitate training. As new systems and technologies are introduced, develop and maintain additional information required.
15. Develop and publish best practices, policies, and procedures on all aspects of the systems environment related to this task area.
16. After all major system/network outages affecting systems/networks within the scope of this task, analyze the factors contributing to the outage, as well as the effectiveness of actions taken to restore services. The Contractor shall publish these analyses and findings in an After Action Report no later than the close of business on the next duty day after restoring the system/network to operational status.
17. Respond to outages, degradations, and HAZCON events for all networks and systems within the scope of this sub-task area IAW USCENTCOM policies, regulations, and procedures.
18. Detect and compile information on recurring problems to determine the effectiveness of corrective actions taken to resolve problem tickets. Recurring problems shall be tracked by problem ticket type (e.g., printing, e-mail, phone, etc.). Analyze the compiled information to identify situations where problem resolution does not provide a stable fix for an issue and suggest COAs to the PM for improving results. Implement COAs selected by the PM and monitor their impact on performance to verify that the frequency of recurring incidents is being reduced. Utilize trend analysis methods and other means to visualize the data.
19. Develop and maintain detailed operational checklists to ensure all Contractor personnel follow standard tactics, techniques, and procedures (TTPs) when preparing for, executing, and validating results of any tasks, processes, authorized service interruptions (ASIs), or maintenance actions impacting services and systems within the scope of this task area. Develop checklist(s) for each task/process identified and ensure Contractor personnel are properly trained to perform the daily operational tasks using the applicable checklist(s). The checklists and associated TTPs shall be made available for review by USCENTCOM.
20. Package, transport, and ship equipment to/from USCENTCOM-supported locations and buildings IAW USCENTCOM logistical support policies, regulations, guidelines, and procedures.

21. Participate in reviews of new systems or modifications of existing systems.
22. Report any temporary changes made to systems and services within the scope of this area within 30 minutes. If the change has the potential for a significant impact, the change shall be coordinated within USCENTCOM prior to implementation.
23. Coordinate internally with other Technical Support Teams and externally with third parties and vendors to troubleshoot outages, service degradations, and HAZCON events and to document fix actions taken to resolve these issues.
24. Install software patches, new releases, and IA updates to ensure all systems and devices within the scope of this task are compliant with applicable STIGs and Security Directives from DMS FoS PMOs and DISA. Ensure all IA updates are applied within required deadlines.
25. Collect any information needed to develop management reports that provide metrics and trend analyses of common problems.
26. Perform site surveys, determine COAs, develop drawings, provide cost and time estimates, generate assembled material lists, and create documentation in support of HQ systems installations and systems infrastructure installations.
27. Manage, maintain, and post a daily Master Station Log (MSL) and shift change procedures to ensure proper information flow across shifts. This MSL shall provide a record of all maintenance requirements, functions, and corrective actions taken. The Contractor shall document when the deficient function and/or operation was first discovered/reported, as well as the exact time it was corrected and when the service, function, and/or operation was restored.

C.5.2.1 C3 System Support

In addition to other tasks described in section C.5.2.1, the Contractor shall provide the following support for all of the tasks/subtasks under the C3 System Support sub-Task Area:

1. Provide infrastructure support for the USCENTCOM Contingency Communications Package (CCP). Support shall include participation in training activities, exercises, and real world deployments. The CCP provides deployable COOP communications capabilities to designated personnel during emergency situations (i.e., hurricanes, fire, flood, cable cuts, power outages, equipment failures, etc.). In the event of a real-world emergency, COOP support could be required for extended periods of time.
2. Prepare and update accreditation packages and maintain accreditation documentation folders for new or existing systems and equipment.

C.5.2.1.1 Management of HQ Systems Infrastructure

Description:
As part of managing the HQ Systems Infrastructure, the Contractor is responsible for the Operations and Maintenance (O&M) of the USCENTCOM Network Infrastructure. This infrastructure includes multiple, disparate Tier 1 and Tier 2 network architectures. The Contractor shall operate, monitor, manage, maintain, install, and troubleshoot USCENTCOM

network infrastructure devices and services within the scope of this task. The Contractor shall support all aspects of network infrastructure management including policies, procedures, implementation, technology integration, and guidance for both scheduled and unscheduled maintenance. Systems, services, and networks within the scope of this task are located at HQ USCENTCOM, multiple locations on MacDill Air Force Base (AFB), Florida, sites within the Tampa Bay metropolitan area, other Continental United States (CONUS) locations, CFH, supported Embassy networks, and other locations within USCENTCOM's AOR.

Activities:
The Contractor shall:

1. Establish and manage a comprehensive Network Infrastructure (NI) Maintenance Program for all networks, systems, and services within the scope of this task. Develop a process/checklist for testing and validating the operational status of network infrastructure systems and services provided to the Command within the scope of this task.
2. Provide dedicated, on-site support for all systems/services/networks operated and maintained by the HQ Systems Infrastructure Technical Support Team.
3. Provide expertise and advice on HQ systems infrastructure to the USCENTCOM Enterprise Operations Center (EOC) via a designated liaison.
4. Baseline and maintain all device configurations (to include software) utilizing Information Assurance (IA) Security Technical Information Guides (STIGs) and maintain configuration control and policy management of all devices within the scope of this task.
5. Develop and publish documentation of lessons learned during troubleshooting, covering best practices, policies, and procedures on all aspects of the systems environment related to this task.
6. Manage the HQ USCENTCOM Internet Protocol (IP) addressing space for all supported networks and all directly supported sites.
7. Collect customer IP addressing requirements and track the fulfillment of these needs.
8. Operate and maintain the USCENTCOM Dynamic Host Configuration Protocol (DHCP) services for all supported networks.

C.5.2.1.2 Voice Services

Description:
The Contractor shall provide maintenance of USCENTCOM's telephony services and associated directorate sub-accounts pertaining to the following:

- Voice Over Internet Protocol (VOIP) phones
- Voice Over Secure Internet Protocol (VOSIP) phones
- VOIP and VOSIP Call Managers
- Perform basic O&M tasks on the Avaya CS-1000M Time Domain Multiplexer (TDM) voice switch servicing USCENTCOM HQ's Secure Telephone Equipment (STEs)

- Omni Encryptors

The Contractor shall maintain property accountability for all phone systems and equipment list above, as well as serve as a focal point for all Telephone Control Officers (TCOs). The Contractor shall train new TCOs as required.

The Contractor shall be responsible for the preparation, configuration, testing, training, issuance, and receipt of STE, OMNI and VOIP/VOSIP devices. This includes activities such as troubleshooting and performing minor repairs on STEs, OMNIs and VOIP/VOSIP phones. The Contractor shall establish and maintain asset inventory management of all telephony devices, STEs, and OMNIs. The Contractor is also responsible for monitoring the usage of telephony services to include the review/audit/reconciliation of usage logs. Additionally, the Contractor shall coordinate the installation of VOIP/VOSIP telephones.

The Contractor shall operate, monitor, maintain, install, and troubleshoot USCENTCOM telephony devices and services at sites designated by USCENTCOM, including, but not limited to, HQ USCENTCOM, multiple sites on MacDill AFB and CFH, and locations within USCENTCOM's AOR.

Activities:

The Contractor shall perform the following on-site support IAW USCENTCOM policies, regulations, and guidance and in locations specified within the scope of this task:

1. Provide dedicated, on-site coverage Monday–Friday from 0700 to 1700 for all systems/services operated and maintained by the Voice Services Technical Support Team. On-call support shall be provided during non-duty hours. The maximum time for reporting to duty station after on-call support is requested is one hour from the time of notification. A comprehensive on-call/alert roster shall be maintained and updated on a monthly basis.
2. Take actions necessary to operate and maintain (O&M) telephony services and devices associated with the TDM telephone system, excluding O&M of the CS-1000 telephone switch.
3. Install / maintain/remove telephony services in the quarters of the USCENTCOM Commander and Deputy Commander.
4. Install / maintain / remove telephony services in the quarters of other USCENTCOM General Officers (GO)/Flag Officers (FO).
5. Install, configure, and maintain USCENTCOM VOIP and VOSIP Call Managers at HQ USCENTCOM and CFH facilities.
6. Install, configure, and maintain VOIP and VOSIP devices IAW USCENTCOM policies, regulations, and procedures.
7. Maintain USCENTCOM telephone accounts and associated directorate sub-accounts pertaining to VOIP, VOSIP, OMNI, and STE devices. The Contractor shall troubleshoot issues with these devices as necessary.
8. Provide support for DoD IT services at embassies within the scope of this task.

9. Manage, maintain, and post a daily MSL and shift change procedures to ensure proper information flow across shifts. This MSL shall provide a record of all maintenance requirements, functions, and corrective actions taken. The Contractor shall document when the deficient function and/or operation was first discovered/reported, as well as the exact time it was corrected, and when the service, function, and/or operation was restored.
10. Monitor voice circuits and devices to facilitate the early detection of incidents, impending outages, or degradations.
11. Validate directorate's monthly phone bills and spot check other directorates' phone bills on a monthly basis to ensure their designated TCOs are properly checking for abuse.
12. Verify and update the Telephone Subscriber Database to include, but not limited to, numbers, subscribers, and port assignments.
13. Update and publish the USCENTCOM Plain Old Telephone System (POTS), Defense Switched Network (DSN), VOIP, and VOSIP Telephone Directories.
14. Perform Annual Telecommunications and Monitoring Assessment Program (TMAP) inspections. Publish TMAP reports documenting findings and recommendations annually.

C.5.2.1.3 Patch and Test Facility (PTF) Support

Description:
The PTF is the primary service delivery point at HQ USCENTCOM for fixed long-haul communication infrastructure services. PTF contractors support USCENTCOM communication requirements and C4 initiatives. PTF team members are responsible for restoring services in accordance with local and higher level policy. The Contractor shall operate and maintain USCENTCOM fixed and deployable IT systems to include transmission systems, hardware, and software associated with long-haul communications systems and tactical network infrastructure equipment. The primary places of performance for this task are HQ USCENTCOM and CFH. Other supported locations include multiple sites on MacDill AFB and within the Tampa Bay metropolitan area, other CONUS locations, locations within USCENTCOM's AOR and other supported Combatant Command (COCOM) AORs. USCENTCOM may require Contractor personnel to travel to remote locations throughout the USCENTCOM AOR in order to perform the activities listed below.

Activities:
The Contractor shall:

1. Provide dedicated, on-site technical support for all circuits/systems/services operated and maintained by the PTF Technical Support Team.
2. Provide expertise and advice on Patch and Test Facility to the USCENTCOM EOC via a designated liaison.
3. Maintain 100% accountability of all tools, test equipment, and other assets within the scope of this task at the beginning of each shift change. Accountability shall be annotated in the MSL.

4. Track and provide budgeting, forecasting, and consumption rate information in order to best utilize and manage spare equipment and ensure all necessary repair parts are available to quickly return assets to operational status.
5. Ensure all scheduled outages for circuits, station lines, systems, and devices within the scope of this task are identified, coordinated, and reported IAW USCENTCOM policies, regulations, and guidelines and Defense Information Systems Agency (DISA) Circular (DISAC) 310-70-1.
6. Document all outages that directly affect GO/FO communications in the Incident Management System regardless of length of the outage.
7. Acknowledge the outage and open a trouble ticket within timelines established in DISA circulars once notified of an outage by USCENTCOM, DISA, or other pertinent agency.
8. Open a new record for outages that originate outside of USCENTCOM or affect users that are unable to record an outage in the Incident Management System and cannot be resolved after ten minutes.
9. Coordinate station qualification, to include developing test criteria, for PTF contractor personnel IAW local USCENTCOM policies, regulations, and procedures as well as DISAC 310-70-1 Para C2.10.1.
10. Ensure that all Contractor personnel are adequately trained on topics covered in DISAC 310-70-1 Chapter 2, paragraphs 9 and 10 in order to perform the daily operational tasks.
11. Complete a circuit history folder review for all circuits traversing the PTF on an annual basis.
12. Manage, maintain and post a daily MSL IAW DISAC 310-70-1 and shift change procedures to ensure proper information flow across shifts. This MSL shall provide a record of all maintenance requirements, functions, and corrective actions taken. The Contractor shall document when the deficient function and/or operation was first discovered/reported, as well as the exact time it was corrected, and when the service, function and/or operation was restored.
13. Monitor circuits and networks within the scope of this task to assess their health and to facilitate early detection of incidents, impending outages, or degradations. On an hourly basis, walk through and thoroughly inspect all USCENTCOM PTFs, and any other facilities, to ensure all equipment is operating correctly, including environmental systems. Any deficiencies noted during the inspection shall be annotated on the MSL. Corrective action shall be taken/requested and the incident shall be tracked until system outages and/or facility deficiencies are repaired or corrected.
14. Support the day-to-day operations of the PTF by performing tasks such as reporting circuit status information, troubleshooting circuit outages, and maintaining operating logs IAW applicable DISA standards.
15. Determine the methodology for restoration of communication services to include moderate equipment configuration changes or modifications within the PTF. The Contractor shall maintain connection services between the user and Wide Area Network (WAN) equipment. Local connectivity may include fiber optic/copper cabling, connectors, and other ancillary devices (e.g., line drivers, modems, Channel Service Units (CSUs)/Data Service Units (DSUs)) required to provide end user services.

16. Troubleshoot and repair interfaces on technical control equipment to include, but not limited to, the following interfaces: RS-449/422, RS-530, RS-232, and Conditioned Diphase (CDI).
17. Provide fault isolation and restoration of strategic, base, and tactical communications circuits/systems to include, but not limited to, voice, video, data, radio, fiber optic, satellite, and command and control information networks.
18. Identify, troubleshoot, and resolve C4 compatibility issues between deployed tactical assets and fixed components.
19. Program, load, maintain, and account for all cryptographic equipment within the scope of this task in accordance with applicable Air Force, DoD and U.S. Government guidance.

C.5.2.1.4 Cable Plant Support

Description:
The Contractor shall provide the engineering, installation, testing and maintenance of the secure/non-secure voice, video, data, and radio frequency cable infrastructure at HQ USCENTCOM, multiple locations on MacDill AFB, sites within the Tampa Bay metropolitan area, other CONUS locations, CFH, and locations within USCENTCOM's AOR.

The Contractor shall perform its work in accordance with the National Electric Contractors Association (NECA)/Building Industry Consulting Service International (BICSI) 568 standard which defines minimum requirements and procedures for installing telecommunications cable infrastructure, including balanced twisted-pair copper cabling and fiber optic cabling. This standard also describes professional workmanship.

Activities:
The Contractor shall:

1. Provide dedicated, on-site coverage Monday through Friday from 0700 to 1800 for all cabling maintained by the Cable Plant Technical Support Team. On-call support shall be provided during non-duty hours. The maximum time for reporting to duty station after on-call support is requested is one hour from the time of notification. The Contractor shall maintain a comprehensive on-call/alert roster and update this roster on a monthly basis.
2. Maintain cable infrastructure labeling standards IAW USCENTCOM developed policies, regulations, and procedures.

C.5.2.2 Enterprise Network Services Support

In addition to other tasks described in section C.5.2.2, the Contractor shall provide the following support for all of the tasks/subtasks under the Enterprise Network Services Support sub-Task Area:

1. Provide on-site dedicated support for systems/services operated and maintained by the Server Maintenance Team, the Communications Center Technical Support Team, the GCCS Technical Support Team, and End-User Information Technology (IT) System Support Team for all computer systems, PEDs, peripherals, hardware devices, and portable, deployable, end-user equipment in support of the USCENTCOM mission (e.g., Secure Mobile Cellular Communications System (SMCCS), laptops).
2. Prepare, update, and maintain accreditation packages for new or existing systems and equipment.
3. Maintain and publish current network information to include trend analysis of common problems and system performance, average device and service uptime, service outage durations and frequencies, trouble ticket status updates, and other parameters identified by the PM.
4. Monitor servers, applications, and services to facilitate early detection of incidents, impending outages or degradations.
5. Determine COAs, develop drawings, provide cost and time estimates, generate assembled material lists, and create documentation in support of GCCS installations, End-User IT System installations, Wireless Communications installations..
6. Develop and publish best practices, policies, and procedures on all aspects of the DMS Family of System (FoS) environment, the GCCS FoS environment related to this task.
7. Support all USCENTCOM Contingency Operations, to include initial installations at Component sites in support of these operations.
8. Manage, maintain, and post a daily MSL and shift change procedures to ensure proper information flow across shifts. This MSL shall provide a record of all maintenance requirements, functions, and corrective actions taken. The Contractor shall document when the deficient function and/or operation was first discovered/reported, as well as the exact time it was corrected, and when the service, function, and/or operation was restored.

C.5.2.2.1 Communications Center

Description:

The contractor shall operate a Communications Center for USCENTCOM. This consists of managing command and control systems that support HQ USCENTCOM and CFH. The systems supported include the Automated Message Handling System (AMHS), Top Secret Collateral (TS/C) Decision Agent Client, Certificate Authority Workstation (CAW), Directory Service Agent (DSA) servers, Administrative Directory User Agents (ADUA), Symantec Backup Exec with tape library, AMHS Lab suite, and the Secure Messaging and Remote Terminal (SMART). The Contractor shall provide support to Special Operations Command, Central (SOCCENT), and U.S. Marine Corps Central Command (MARCENT) by managing their Defense Message System (DMS) directory entries. The Contractor shall also manage a COMSEC sub-account and COMSEC key updates for communications circuits.

Activities:

The Contractor shall:

1. Operate and manage a garrison Defense Messaging System. This includes, but is not limited to, hardware and software for the AMHS/CPXP Servers (2), (DSA (2), ADUAs (6), CAW (2), TS/C Decision Agent Client (1), and peripheral equipment. DMS components, such as the CAW, require the Operator/Administrator to be certified through formal training.
2. Operate and manage a deployed DMS messaging system at CFH (Qatar) in support of exercises, disasters, and COOP. The deployable suite includes AMHS/CPXP servers (2), DSA (2), ADUAs (4), TS/C Decision Agent Client (TS/C) (1), domain controllers, and peripheral equipment.
3. When requested by the Joint Area Control Center, administer systems for the Joint Regional AMHS located in HQ USCENTCOM, MacDill AFB.
4. Coordinate software maintenance to include troubleshooting, testing, applying Field Engineering Notes (FENs), software updates and IA updates IAW DMS Program Management Office direction.
5. Monitor and respond to service messages, directory scan reports, and DISA Interim Procedures.
6. Provide DMS software and hardware configuration control and licensing accountability by developing and maintaining a DMS software and hardware configuration control and licensing repository.
7. Provide notification and routing of hardcopy special category and top secret message traffic to appropriate organizations IAW USCENTCOM policies, regulations, and guidelines and based on message precedence. This includes telephone notification, electronic mail, logging, and receipt.
8. Maintain complete chain of custody logs for special category (SPECAT) messages.
9. Complete daily, weekly, monthly, quarterly, and yearly cryptologic changeovers and updates IAW USCENTCOM policies, regulations, and guidelines.
10. Provide a certified COMSEC Responsible Officer (CRO) and alternate within 14 calendar days of TO award. This CRO shall manage all COMSEC material and keys assigned to the sub-account, prepare for command and Major Command (MAJCOM) inspections, account for COMSEC documents, and conduct training for all personnel with authorized access.
11. Provide a certified Certificate Authority (CA) and alternate person to manage and generate X.500 certificates using the CAW IAW with DoD Certificate Policy, dated 4 May 2011 and AF Certificate Practice Statement v2.0.1.
12. Prepare for Defense Messaging System-Air Force (DMS-AF) Program Management Office (PMO) inspections and NSA audits.
13. Prepare unclassified and classified message systems for deployments.
14. Maintain DMS detailed designs for normal operations, as well as in support of exercises and real world contingencies.
15. Notify the PM of proposed and approved DMS PMO baseline changes as they relate to USCENTCOM.
16. Manage DMS directory entries on behalf of SOCCENT and MARCENT.

C.5.2.2.2 Global Command and Control System (GCCS) Support

Description:
The Contractor shall be responsible for ensuring system availability and reliability of the Global Command and Control System - Joint (GCCS-J) and related GCCS FoS on U.S. and Coalition networks at HQ USCENTCOM and CFH. The Contractor shall provide technical support to USCENTCOM and all USCENTCOM Joint Task Force (JTF) and service components in the AOR. The Contractor shall plan, develop, and implement GCCS program requirements. The Contractor shall be responsible for maintenance, troubleshooting, installation, configuration, and the implementation of existing and future versions of the GCCS FoS.

The Contractor shall provide system administration support, technical support, and subject matter expertise for GCCS FoS, including:

- Common Operational Picture (COP)
- Integrated Imagery and Intelligence (I3)
- Joint Operation Planning and Execution System (JOPES)
- Command and Control Personal Computer (C2PC)
- Information Assurance (IA) and Client/Server installation
- Theater Air Missile Defense (TAMD) and various GCCS-J subsystems

Activities:
The Contractor shall:

1. Provide management, system administration, planning, and operational support for all Command and Control servers and client assets, including UNIX systems, within the scope of this task.
2. Serve as the alternate Functional Manager (FM) and subject matter expert for JOPES.
3. Directly administer GCCS FoS assets employed at HQ USCENTCOM, and provide technical support to deployed units in USCENTCOM's AOR.
4. Perform Configuration Management and Project Management and ensure IA compliance for all USCENTCOM GCCS FoS assets.
5. Perform any necessary actions required to respond to GCCS FoS problem reports.
6. Perform system, security, and operational testing/evaluation events in coordination with Joint Staff (JS) J3 and GCCS-J PMO to determine suitability to field for future releases.
7. Ensure USCENTCOM personnel and Contractors are trained on the GCCS FoS server-based systems and maintain a recurring training program.
8. Manage and administer the Radiant Mercury Cross Domain Solution (CDS) or other designated CDS in support of the USCENTCOM GCCS mission.

C.5.2.2.3 End-User Information Technology (IT) System Support

Description:

The Contractor shall provide O&M support for client computing devices to include personal computers, thin clients, laptops, Portable Electronic Devices (PEDs) and peripherals located at HQ USCENTCOM, CFH, and Bahrain. For all computer systems, peripherals, and other hardware devices within the scope of this task, the Contractor shall establish a technical support program to install, maintain, upgrade, replace, and in the event of a failure or degradation in performance, analyze, troubleshoot, and restore systems/devices to operational status. The Contractor shall coordinate and manage all equipment installations within the scope of this task. Systems and networks within the scope of this task are located at HQ USCENTCOM, multiple locations on MacDill AFB, sites within the Tampa Bay metropolitan area, other CONUS locations, CFH, and locations within USCENTCOM's AOR.

Activities:
The Contractor shall:

1. Provide end-user IT system and software maintenance for the USCENTCOM CCP. This support shall include participation in training activities, exercises, and real world deployments. The CCP provides deployable COOP communications capabilities to designated personnel in support to new missions and during emergency situations (i.e., hurricanes, fires, floods, cable cuts, power outages, equipment failures, etc.). In the event of a real-world emergency, COOP support could be required for extended periods of time.
2. Coordinate and manage Automated Data Processing Equipment (ADPE) accountability of new equipment, replacement equipment, and upgrades. The Contractor shall also track the disposition of equipment throughout its life cycle (e.g., Computer Equipment Replacement Program (CERP) and Life Cycle Replacement (LCR)).
3. Process end of life, defective, and/or damaged equipment through the Defense Reutilization Management Office (DRMO).
4. Develop procedures to facilitate management and testing of desktop load set configurations to include tracking and compiling of user issues, software conflicts, devices conflicts, and other similar tasks.
5. Provide support the Very Important Person (VIP) team. VIPs consist of local quarters, office and travel to CONUS and Outside the CONUS (OCUNUS) locations.
6. Support VIP Communication / Information Systems and networks, including remote communications equipment, mobile and deployable network communication systems, strategic and tactical multi-channel satellite communication systems (BGAN terminals), secure telephone equipment, video conferencing terminals, laptops, desktops, computer peripherals and other equipment, supporting executive communications capabilities.
7. Test all VIP deployable mobile communications equipment and communications suites to ensure all equipment is operational. The equipment shall be ready to deploy within one hour of the notifications for deployment.

C.5.2.2.4 Server Maintenance Support

Description:

A robust Server Maintenance program ensures that key and supporting services are reliable and available to end users when needed. As such, the Contractor shall establish and operate a Server Maintenance program that provides systems administration, maintenance, computer security, and support for servers on all USCENTCOM networks, as well as those at SCO locations throughout the USCENTCOM AOR and those on Allied and Coalition networks. The Contractor shall also operate and maintain items such as servers (physical and virtual), firmware, operating systems, software, and Storage Area Networks (SANs). Systems and networks within the scope of this task are located at HQ USCENTCOM, multiple locations on MacDill AFB, sites within the Tampa Bay metropolitan area, other CONUS locations, CFH, and locations within USCENTCOM's AOR.

Activities:

The Contractor shall:

1. Provide robust and secure day-to-day operations by maintaining, managing, monitoring, and administering server systems on USCENTCOM, Allied/Coalition, and SCO-based networks.
2. Maintain and administer all hardware, software, firmware, and operating systems for all systems within the scope of this task.
3. Provide support for DoD IT services at U.S. Embassies within the scope of this task.
4. Perform capacity planning and allocate disk space.
5. Provide server support for the USCENTCOM CCP. This support shall include participation in training activities, exercises and real world deployments. The CCP provides deployable COOP communications capabilities to designated personnel in support to new missions and during emergency situations (i.e., hurricanes, fires, floods, cable cuts, power outages, equipment failures, etc.). In the event of a real-world emergency, COOP support could be required for extended periods of time.
6. Advise USCENTCOM regarding any required modifications or upgrades to server equipment and software.
7. Monitor servers, applications, and services to facilitate the early detection of incidents, impending outages, or degradations.
8. Provide server IA (i.e., Information Assurance Vulnerability Alert (IAVA) assessment compliance), health (e.g., disk and central processing unit (CPU) utilization) and status reports to the PM.
9. Ensure that the IT environment is accessible through the establishment and maintenance of user accounts, profiles, print and disk services, data file services, Domain Name services, and other means.
10. Provide aggressive computer security management to maximize server security posture. Monitor and review computer security scans, intrusion detection reports, and implementation of security upgrades and applications.
11. Configure, manage, and maintain the USCENTCOM thin client architecture on all networks and systems within the scope of this task IAW USCENTCOM policies, regulations, and procedures.
12. Configure, manage, and maintain the USCENTCOM boundary security devices and architecture on all networks and systems within the scope of this task IAW USCENTCOM policies, regulations, and procedures.

13. Configure, manage, and maintain the USCENTCOM virtual computing infrastructure on all networks and systems within the scope of this task IAW USCENTCOM policies, regulations, and procedures.
14. Provide expertise and advice on server operations and maintenance to the USCENTCOM EOC via a designated liaison.
15. Provide the following documentation:
    - Inventory of all assets and spare equipment
    - Prioritized Service Restoration List
    - Server Maintenance Physical and Logical Diagrams of systems and their associated storage for all USCENTCOM networks
    - Operational Checklists documenting standard tactics, techniques and procedures (TTPs) for executing tasks required to support server operations.
    - Consolidated folder of best practices, policies and procedures.
    - Server Security Report (including IAVA compliance status information).
    - Server Health Report
    - Server Status Report

C.5.2.2.5 Wireless Communications

Description:
The Contractor shall establish and manage a comprehensive Wireless Communications Program at HQ USCENTCOM, CFH, and USCENTCOM offices at the Pentagon and Bahrain. Users on travel both within the CONUS and the USCENTCOM AOR shall be supported. The Contractor shall provide all aspects of program maintenance, including the drafting of policies and procedures and the implementation and integration of new wireless services and technologies, as well as troubleshooting, repair, and logistical support for existing devices. Systems and networks within the scope of this task are located at HQ USCENTCOM, multiple sites on MacDill AFB and within the Tampa Bay metropolitan area, other CONUS locations, CFH, and locations within USCENTCOM's AOR.

The Contractor shall manage secure and non-secure wireless communications devices and associated auxiliary devices, wireless access points / controllers, and other user-operated wireless/auxiliary devices providing either network or cellular connectivity.

Activities:
The Contractor shall:

1. Provide dedicated, on-site customer support coverage Monday – Friday from 0600-1800 for all systems/services operated and maintained by the Wireless Communications Technical Support Team. On-call support shall be provided during non-duty hours. The maximum time for reporting to duty station after on-call support is requested is one hour from the time of notification. A comprehensive on-call/alert roster shall be maintained and updated on a monthly basis.

2. Provide a primary and alternate Personal Wireless Communications Manager (PWCS) IAW USCENTCOM Regulation 105-7; maintain a current list of these POCs and update the list as changes occur.
3. Prepare, configure, test, troubleshoot, issue, and receive wireless communications devices and associated auxiliary devices.
4. Manage all billing related to wireless communications devices, auxiliary devices, and services within the scope of this task.
5. Interface directly with customers to provide training and to resolve all issues related to services within the scope of this task.
6. Maintain utilization history to include review of device/service usage, audits, and reconciliation of utilization.
7. Provide primary and alternate Personal Wireless Communications Manager (PWCS) documentation
8. Maintain records on monthly billing and notices to Directorates/customers.
9. Provide USCENTCOM with monthly cell phone billing analysis that includes recommendations for reducing costs.
10. Maintain and periodically test two complete suites of deployable communications equipment, packed in the appropriate transit cases in accordance with work center instructions. At least one suite of deployable communications equipment shall be available to deploy within 5 hours of notification and shall be completely tested to verify operational status within 3 hours of notification.

C.5.2.3 Operations Support
In addition to other tasks described in section C.5.2.3, the Contractor shall provide the following support for all of the tasks/subtasks under the Operations Support sub-Task Area:

C.5.2.3.1 Visual Information Services (VIS)

Description:
The Contractor shall provide and support Visual Information Services (VIS) which includes, but is not limited to, the setup, adjustment, and operation of video teleconferencing (VTC) devices, teleconferencing services, audio-visual (A/V) services, desktop collaboration services, public address (PA) systems and multi-display clocks. The Contractor shall provide robust VIS capabilities for HQ USCENTCOM and CFH meeting and conference facilities, as well as public events as required. The Contractor shall support these services on Non-secure Internet Protocol Router Network (NIPRNet), Secret Internet Protocol Router Network (SIPRNet) and Combined Enterprise Regional Information Exchange Service(CENTRIXS or CIX)-International Security Assistance Force (CENTRIXS-ISAF).

Activities:
The Contractor shall:

1. Provide dedicated, on-site end user support for mission critical and mission essential VIS systems/services operated and maintained by the VIS Technical Support Team. The Contractor shall support all events outside of duty hours.

2. Integrate, test, maintain, and operate VTC and A/V suites and teleconferencing hardware and software.
3. Establish USCENTCOM VTC and A/V connectivity to other locations and equipment.
4. Schedule, coordinate, and administer multiple simultaneous VTC and A/V sessions.
5. Ensure that all PA systems and associated equipment are operational and capable of supporting events.
6. Support the distribution of Closed Circuit Television (CCTV) within USCENTCOM facilities. The USCENTCOM PM shall determine the number of channels to distribute.
7. Maintain situational awareness of Joint Worldwide Intelligence Communications System (JWICS) VTC capability, report degradations and outages IAW USCENTCOM policy, and provide assistance to correct any problems or issues.
8. Provide advisory support for the USCENTCOM CCP. Support shall include participation in training activities, exercises and real world deployments. The CCP provides deployable COOP communications capabilities to designated personnel in support of new missions and during emergency situations (i.e., hurricanes, fires, floods, cable cuts, power outages, equipment failures, etc.). In the event of a real-world emergency, COOP support could be required for extended periods of time.
9. Recommend upgrades to the VTC and AV systems at least annually and incorporate approved upgrades if/when acquired.
10. Manage, maintain, and post a daily MSL and shift change procedures to ensure proper information flow across shifts. This MSL shall provide a record of all maintenance requirements, functions, and corrective actions taken. The Contractor shall document when the deficient function and/or operation was first discovered/reported, as well as the exact time it was corrected, and when the service, function and/or operation was restored.
11. Monitor VIS services to facilitate the early detection of incidents, impending outages or degradations.
12. Schedule, configure, and connect USCENTCOM users to Defense Video Services (DVS) conferences.
13. Provide Defense Collaboration Online (DCO) end-user support by issuing headsets to new account holders and assist users in the use of the application.
14. Train both USCENTCOM and Contractor personnel on the operation of A/V and VTC equipment.
15. Maintain a COMSEC account for key material necessary to run secure VTCs.
16. Provide customer support for cable and satellite television service requests.
17. Validate cable and satellite television billing.

C.5.2.3.2 Security Cooperation Organization (SCO) Support

Description:
USCENTCOM is required to provide sustained C4 support for 17 SCO Offices located in U.S. Embassies throughout USCENTCOM AOR. The ultimate goal is to ensure data, voice, video, and

communication requirements are correctly provisioned and operational to support assured communication between Commander USCENTCOM and U.S. Ambassadors.

The Contractor shall provide systems integration and installation support to 17 SCOs located in U.S. Embassies throughout USCENTCOM AOR. The Contractor shall administer systems, perform testing, perform training, and provide O&M support for computers, voice, video and communications at each SCO. The Contractor shall utilize remote communications (e.g., electronic mail, telephone), as well as site visits to accomplish this task.

Activities:
The Contractor shall:

1. Provide remote support for all system/services operated and maintained within the scope of this task at SCO locations, without any on-site technical support. On-call support shall be provided outside of these hours, with a maximum time for reporting to duty station after on-call support is requested of one hour from time of notification. The Contractor shall maintain a comprehensive on-call/alert roster and update this roster on a monthly basis.
2. Procure, install, configure, and maintain SCO SIPRNet hardware and software.
3. Procure, install, configure, and maintain SCO NIPRNet hardware and software in instances where this service is not provided by the embassy.
4. Install, troubleshoot, repair, operate, and maintain computers, telecommunications, and network equipment to include workstations, servers, printers, scanners, cryptographic encryptors, telephones, and any other equipment within the scope of this task.
5. Provide life cycle management of SCO SIPRNet and NIPRNet equipment IAW USCENTCOM Regulation 25-75, “Information Management Security Cooperation Organization (SCO) Information Systems Support.”
6. Perform site assistance visits of all embassies to maintain 100% accountability of all assets within the scope of this task. Track and provide budgeting, forecasting, and consumption rate information in order to best utilize and manage spare equipment and ensure all necessary repair parts are available to quickly return assets to operational status. Visits shall be scheduled at least once a quarter or as requirements emerge.
7. Provide the IS equipment inventory to USCENTCOM IAW Regulation 25-75.
8. Identify equipment and supply shortfalls to the Branch Chief or their designee.
9. Establish test procedures and perform initial testing of new or upgraded capabilities. Perform periodic testing after installing these capabilities.
10. Research and test new technology/systems to evaluate compatibility with current systems and make implementation recommendations. Assist SCOs in projecting future IS requirements as necessary.
11. Consolidate embassy communications test reports from other organizations into consolidated current status charts.
12. Monitor and test communication systems, networks, applications, and servers to facilitate early detection of incidents or impending outages or degradations IAW

USCENTCOM Regulation 25-75. Coordinate as needed with USCENTCOM and external organizations to monitor and/or test communication capabilities.

13. Report the status of all monitored capabilities IAW USCENTCOM Regulation 25-75.
14. Provide support for all embassy SCO equipment during site visits, to include: account management, software loads, hardware and software maintenance, cable runs, network administration, system administration, and COMSEC loads.
15. Maintain cable infrastructure labeling standards in accordance with USCENTCOM developed policies and procedures.
16. Provide reports, complete requests for new service, and recommend methodologies for installing new or upgraded communications circuits.
17. Draft and staff Request for Service (RFS) correspondence necessary to start, stop, or change network or communications services.
18. Perform system and data backups on SCO systems and servers IAW USCENTCOM back-up policies.
19. Provide user training and assistance on USCENTCOM equipment to all SCO personnel.
20. Update USCENTCOM SCO website to inform users in the AOR about events and important equipment-related information.
21. Assist USCENTCOM in capturing and preserving documents from the SCOs during annual records calls.
22. Provide updates to embassy phone lists.

C.5.2.4 Customer Support Operations (CSO)

Description:

The USCENTCOM Customer Support Operations (CSO) provides a centralized single point of contact for USCENTCOM end users to quickly and easily interface with IT customer service operations. The CSO provides dedicated, on-site support at HQ USCENTCOM and the CFH. The CSO performs troubleshooting of tickets in efforts to resolve issues quickly. The CSO also ensures accurate categorization, prioritization, routing, transfers, and data integrity of all applicable tickets. It ensures consistent incident, change request, problem ticket, and work order life cycle processing.

The CSO interfaces with end-users via telephone calls, automated requests, electronic mail, and other means.

The CSO provides walk-in support for customers at HQ USCENTCOM that have issues requiring face-to-face interaction, such as managing network accounts and resetting Common Access Card (CAC) Personal Identification Numbers (PINs). The CSO supports users on all applicable networks within the scope of this task.

Activities:

The Contractor shall:

1. Provide dedicated, on-site CSO support at HQ USCENTCOM and CFH.

2. Establish and maintain a CSO customer walk-in reception desk at HQ USCENTCOM that operates from during normal duty days as defined by USCENTCOM.
3. Develop a CSO Concept of Operations (CONOPS).
4. Provide Ticket Management support such as troubleshooting, recording, prioritizing, tracking, escalating, and contacting end users.
5. Identify, research, and resolve tickets within the scope of Tier 1 support capabilities. Tickets that require technical support or root cause determination that exceeds Tier 1 support capabilities shall be escalated to higher level support teams for expedient resolution.
6. Monitor and track the status of all incidents, problem tickets, change requests, and work orders submitted, including cases where they are escalated to higher levels of support.
7. Publish a weekly Customer survey analysis report.
8. Recommend proposed fix actions to reverse negative trends. Perform follow-on trend analyses to assess the impact of any fix actions selected by USCENTCOM for implementation.
9. Review, edit, and maintain TTPs for CSO activities to execute and validate results of any tasks and processes within the scope of this task. These TTPs shall be published within 30 calendar days after TO award and updated as changes occur.
10. Identify trends in customer service and technical proficiency; take steps to improve service based on findings.
11. Develop and update the CSO Concept of Operations.

C.5.2.5 Commander Communications Support

Description:

The Contractor shall provide O&M, network engineering and customer support for mobile communications equipment, IS, and networks that support the Commander and Deputy Commander of USCENTCOM and their staff members during travel. The Contractor shall also provide O&M and initial installation support for computer systems, communications, and any other supporting equipment located at the residences of both the Commander and Deputy Commander of USCENTCOM. The Contractor shall provide specific detailed information needed to support the selection of hardware and software and the identification of implementation techniques/tools that provide efficient solutions for meeting current and future business needs. The Contractor shall install, operate, maintain, and in the event of system/network outages, analyze, troubleshoot and repair communications systems, IS, and network equipment to restore them to operational status. Communications/IS and networks that shall be supported include, but are not limited to, remote communications equipment, mobile and deployable network communication systems, strategic and tactical multi-channel satellite communication systems (including KU/GAN/BGAN terminals), secure telephone equipment, video conferencing terminals, laptops, desktops, computer peripherals and other equipment in support of executive communication capabilities. Limited travel to CONUS and Outside the CONUS (OCONUS) locations shall be required.

Activities:

The Contractor shall:

1. Provide dedicated, on-site support for all systems/services/networks operated and maintained by the Commander's Communications Technical Support Team. On-call support shall be provided during non-duty hours and holidays. The maximum time period for reporting to duty station after on-call support is requested is one hour from the time of notification. A comprehensive on-call/alert roster shall be maintained and updated on a monthly basis.
2. Develop and publish best practices, policies, and procedures regarding methods and techniques for packing of equipment that minimize damage during transit.
3. Monitor mobile Commander's Communications Team systems and network connectivity to facilitate early detection of incidents, impending outages, or degradations.
4. Maintain three complete suites of deployable communications equipment for both the Commander and Deputy Commander of USCENTCOM (total six suites), packed in the appropriate transit cases in accordance with work center instructions. The contents of each deployable communications suite shall be determined by the Contractor and validated by the PM. At least one suite of deployable communications equipment for the Commander and one for the Deputy Commander (total two suites) shall be available to deploy within 72 hours of notification and shall be completely tested to verify operational status within 48 hours of notification.
5. Periodically test all deployable communications suites at time intervals determined by the PM to ensure all equipment is operational.
6. Load and unload all communications equipment within the scope of this task on/off airborne assets and vehicles.
7. Provide and assist USCENTCOM with information on systems/equipment needed to support system life cycle replacement planning and execution including procurement of hardware, software, and necessary supplies for the sustainment of equipment and systems.
8. Design and plan mobile and deployable network communications systems.
9. Coordinate with the appropriate agencies to establish reach-back and long-haul circuit interconnections.
10. Coordinate with third party vendors and USCENTCOM Subject Matter Experts (SMEs) to support tasks such as research, development, testing, and pricing of equipment and systems.
11. Provide support to the USCENTCOM CCP. This support shall include participation in training activities, exercises, and real world deployments. The CCP provides deployable COOP communications capabilities to designated personnel in support to new missions and during emergency situations (i.e., hurricanes, fires, floods, cable cuts, power outages, equipment failures, etc.). In the event of a real-world emergency, the Contractor may need to deploy within the USCENTCOM AOR in support of operations, and COOP support could be required for extended periods of time.
12. Install laptop load set configurations including unique user profiles on all relevant mobile kit components within the scope of this task and update and modify these configurations or profiles as needed.

13. Integrate all hardware and software within the scope of this task.

C.5.2.6 Headquarters (HQ) User Training

Description:
The Contractor shall create and manage a customer training program covering IT skills required for end-users at USCENTCOM to effectively perform their duties. The Contractor shall also create and manage a training program covering skills required for technical support teams to effectively perform their duties. Training shall be provided only to Government and Military personnel unless an exception is granted by USCENTCOM and GSA.

Activities:
The Contractor shall:

1. Provide on-site training based on USCENTCOM training requirements at locations designated by USCENTCOM. While the majority of training classes may occur during duty hours (Monday through Friday 0800 – 1700), training may be conducted during the evenings or weekends. In addition, the training location may require the instructor to travel and deliver training to USCENTCOM users or technicians outside the installation.
2. Develop training courses and materials covering topics related to Information Systems (IS), IT, software applications, and other emerging technologies adopted by USCENTCOM.
3. Conduct periodic surveys to assess the training requirements of customers and provide a recommended curriculum for each quarter to the PM for consideration.
4. Based on the curriculum selected by USCENTCOM, update the training program on a quarterly basis to keep pace with changes in requirements. The training curriculum shall be implemented within five duty days after the start of each quarter.
5. Train USCENTCOM personnel on Command standard software applications, designated IS, and other subject areas.
6. Determine if students require follow-on training in order to execute required tasks associated with system use and maintenance based on guidance from the PM or senior leadership.
7. Support Division training meetings in order to obtain training requirements and identify training gaps that prevent technicians or end-users from performing their duties.
8. Conduct courses utilizing new or revised material for trial group(s) of USCENTCOM personnel.
9. Develop training schedules.
10. Schedule students for classes and keep attendance records for all classes taught by the Contractor
11. Track and provide budgeting, forecasting, and consumption rate information in order to best utilize and manage training materials.
12. Develop, collect, and archive Course Customer Satisfaction Surveys to measure and perform trend analyses of the effectiveness of courses and instructors.

C.5.3 TASK AREA 3 – THEATER NETWORK OPERATIONS (NetOps) SUPPORT

The Contractor shall comply with the appropriate DoD-approved architectures, programs, standards, and guidelines, such as Global Information Grid (GIG), Strategic Technical Guidance (STG), Defense Information Infrastructure (DII) Common Operating Environment (COE), Defense Information Systems Network (DISN) and Shared Data Environment (SHADE). Specific services addressed in this PWS are: Level 0 Fault Monitoring, Identification, Resolution; Level 1 Current Operations Support; and IA/Computer Network Defense to the command.

C.5.3.1 Level 0 Fault Monitoring, Identification, Resolution

The Contractor shall be responsible for providing real-time, operational configuration management and control of the GIG/TIG transmission; author, update, and disseminate Trouble Management Ticket reporting; coordinate, generate, direct, and staff authorized service interruptions to ensure state of health of the GIG/TIG networks; ensure timely and accurate status reporting for all GIG/TIG links, trunks, circuits, and other systems to deliver the combatant component agencies across USCENTCOM AOR; reconcile outages/degradation/HAZCON reporting discrepancies between the various reporting agencies; and update and disseminate communications status reports.

The Contractor shall:

1. Provide dedicated, on-site support.
2. Detect current status and state change of select Tier 0, Tier 1, and select Tier 2 network devices (current configuration and up/down).
3. Detect current status and state change of "Core" application services.
4. Correlate events of network devices and applications for system status.
5. Monitor logical network topology (connectivity and routing).
6. Evaluate and respond to event triggers.
7. Monitor network device and application performance.
8. Coordinate and prioritize changes for theater backbone (Tier 0, Tier 1, and select Tier 2 systems).
9. Execute approved changes, responses, corrective actions (where USCENTCOM has change authority); coordinate approved changes where component has change authority.
10. Receive and assemble data to assess impacts to operations/intelligence/business missions by correlating operational events with reported network status and assess and report network event effects (what is up/down/available) and impact (network/operational capability lost/remaining).
11. Generate reports using ticketing system (primary), email, phone, web portal posting, message traffic, and database entry.
12. Record and archive reports and store for trend analysis.

13. Format and disseminate reports to higher, peer, and subordinate Network Operations (NetOps) Centers.
14. Perform trend analysis for performance and security events on Tier 0, Tier 1 devices, and associated connectivity.
15. Validate configurations for Tier 0, Tier 1, and select Tier 2 devices and applications.
16. Escalate events/issues to appropriate Level 1 operators.

C.5.3.2 Level 1 Current Operations

The Contractor's duties and responsibilities include providing current operations support and expertise for voice, data, transmission, and video support and liaison between Combatant Commander, United States Cyber Command (USCYBERCOM), USCENTCOM Components, and JTFs; maintaining situational awareness of USCENTCOM AOR network performance and assisting Components and JTFs with operational issues; maintaining network diagrams; and assisting with NetOps reporting

The Contractor shall:

1. Maintain situational awareness of Tier 0, Tier 1, and select Tier 2 network networks and perform proactive network element status and health checks.
2. Maintain situational awareness of the USCENTCOM Tier 1 transmission network issues and performance.
3. Identify transmissions network problems. Ensure strategic-to-tactical transmissions connectivity is functioning properly.
4. Advise the Watch Officers and Operations Officer on the robustness and performance of the theater transmissions architecture and recommend courses of action if required.
5. Assist components and JTFs with transmissions and troubleshooting of issues.
6. Monitor and evaluate configurations and performance of the Tier 1 transmissions network.
7. Assist in the reporting of transmission issues.
8. Maintain transmissions network diagrams.
9. Ensure commercial connectivity is functioning properly.
10. Upon receipt of escalated network trouble conditions, implement network recovery procedures to isolate specific trouble source.
11. Coordinate corrective actions to restore and repair network condition internally and externally.
12. Initiate, update, track, and close USCENTCOM-approved trouble tickets.
13. Respond to requests for technical support from elements deployed in the USCENTCOM AOR.
14. Document, track, and monitor problems to ensure timely resolution.
15. Execute effective actions to meet mean time to repair and network availability goals and objectives.
16. Process, validate, and determine impacts of Satellite Access Request (SAR)/Gateway Access Request (GAR) for connectivity.
17. Participate in engineering DCOs and NetOps conferences.

18. Monitor logical network topology (connectivity and routing).
19. Monitor network device and application performance.
20. Receive and assemble data to assess impacts to operations/intelligence/business missions by correlating operational events with reported network status and assess and report network event effects (what is up/down/available) and impact (network/operational capability lost/remaining).
21. Generate reports using ticketing system (primary), email, phone, web portal posting, message traffic, and database entry.
22. Analyze configurations for Tier 0, Tier 1, and select Tier 2 devices and applications to correct network anomalies.
23. Provision/allocate resources for validated requirements on Satellite Communications (SATCOM) bandwidth, SATCOM channels, router ports, multiplexer ports, and dedicated circuits.
24. Control access to network resources and devices.
25. Implement network and security access policy; access to resources granted through technical means.
26. Implement NetOps constructs and policies for USCENTCOM.
27. Correlate events of network devices and applications for system status.
28. Coordinate and prioritize changes for theater backbone (Tier 0, Tier 1, and select Tier 2 systems).
29. Execute approved changes, responses, and corrective actions (where USCENTCOM has change authority); coordinate approved changes where component has change authority.
30. Exercise COOP capability if required.
31. Respond to outage or event (reporting, coordinate changes, apply security patches, coordinate network minimization, etc.).
32. Record and archive reports and store for trend analysis.
33. Format and disseminate reports to higher, peer, and subordinate NetOps Centers.
34. Provide basic analysis and identify issues for performance and security event trends for Tier 0, Tier 1 devices, and associated connectivity.
35. Provide basic network optimization analysis (network improvement to optimize traffic and performance) and identify issues for detailed analysis by engineering cell.
36. Perform fault analysis–impacts to user and network performance based on predictive or actual network (or security) faults.
37. Provide network analysis data to support engineering COA development and increase understanding of network, user, and Net Defense impacts.
38. Provide tracking and coordination of intra/inter theater ASIs throughout the AOR.
39. Process component ASI requests and track all ASIs from initial requests to completion.
40. Provide ASI impact assessments of network systems, provide resolution to components with conflicting resources, and make recommendations to the Chief Watch Officer to assist in the approval process.
41. Verify ASI front page for Commander’s Critical Information Requirements (CCIR) status and reporting, complete ASI trouble tickets using USCENTCOM approved systems to provide reports for situational awareness, and brief ASI status to Theater NetOps Center (TNC) Operations Chief.

C.5.3.3 Information Assurance – Computer Network Defense (CND)

The Contractor shall:

1. Provide dedicated, on-site support.
2. Create and deliver the daily IA-CND Current Operations Brief for the J6 and Operations staff.
3. Provide escalation support (Tier III) to IA-CND Current Operations Watch Officers or other NetOps Center or IA staff member.
4. Review IA-CND current operations trends to identify anomalies for further investigation.
5. Manage theater Information Assurance Vulnerability Management (IAVM) program; supervise tracking and reporting of current theater IAVA status.
6. Maintain and update IA-CND Current Operations TTP/SOP.
7. Provide expert IA-CND advice and expertise to USCENTCOM in support of incident handling, course of action development, and related IA-CND response actions.
8. Develop and implement a training program to maintain the knowledge, skills, and abilities of IA-CND Current Operations Watch Officers and ensure familiarity/adherence to IA-CND Current Operations TTP/SOP.
9. Maintain and deliver IA-CND Current Operations Watch Officers schedule.
10. Coordinate the integration of IA-CND current operations activities with other NetOps current operations within the USCENTCOM NetOps Center.
11. Coordinate the integration of IA-CND current operations activities with IA-CND intelligence activities to support intelligence-operations synchronization.
12. Recommend changes to policy, procedure, or technology relevant to improvement of theater IA-CND posture and capabilities.
13. Coordinate theater collaboration for IA-CND planning and operations including chat, ticketing, and collaboration session communications.
14. Provide SME support to Operational Planning Teams and planning tasks assigned to the IA-CND Branch; respond to JS and USCENTCOM taskers and Requests for Information (RFIs) (with Government approval).
15. Provide IA-CND Current Operations Watch (24x7 operations coverage for Event Handling and Situational Awareness)
16. Perform real-time analysis of theater IA-CND data from appropriate situational awareness and management tools, to include, but not limited to:
    - ARCSIGHT data analysis and queries.
    - Host-Based Security System (HBSS) monitoring, configuration, and reports/queries.
    - User Defined Operational Picture (UDOP) monitoring of national and theater IA-CND information.
    - Theater Network Management Architecture (TNMA)-related tools for IA-CND specific information queries and analysis.
17. Perform information gathering from appropriate tools and databases, to include, but not limited to:
    - CENTAUR queries.

- BLUESASH queries.
- USCENTCOM-specific information databases.

18. Receive and track theater Firewall Exception Requests (FER).
19. Coordinate theater collaboration for IA-CND planning and operations including, but not limited to, email, chat, ticketing, and collaboration session communications.
20. Participate in GIG collaboration for IA-CND current operations including, but not limited to, email, chat, ticketing, and collaboration session communications.
21. Coordinate theater IA-CND trouble ticket management.
22. Coordinate theater IA-CND RFI management for routine and event-related requests.
23. Maintain IA-CND sensor grid situational awareness from Tier 0 to Tier 2; report and respond to sensor grid outages and/or anomalies; coordinate network surveillance resources.
24. Track and report theater IA-CND performance/capability metrics.
25. Disseminate IA-CND and relevant Operational Security (OPSEC) reports/data.
    - Classified material incidents.
    - Joint COMSEC Monitoring Agency reports.
    - Information Operations Condition (INFOCON) changes.
    - Communication Tasking Order (CTO)/USCENTCOM Communications Tasking Order (CCTO)/Operational Directive Message (ODM) dissemination, tracking, and compliance monitoring and coordination.
26. Coordinate Theater Information Grid (TIG) and GIG event handling and response actions.
27. Coordinate and manage INFOCON changes and track compliance.
28. Review IA-CND current operations trends to identify anomalies for further investigation.
29. Report CCIRs, Priority Intelligence Requirements (PIRs), other information requirements IAW USCYBERCOM, USCENTCOM, CCJ6 and Information Assurance Management (IAM) requirements and IAW SOP/TTPs.
30. Review current intelligence for relevant threats and develops appropriate actions/response.
31. Distribute current IA-CND intelligence information to the USCENTCOM Components.
32. Provide relevant information to Theater IA-CND Intelligence Section for threat analysis and response support.
33. Integrate IA-CND current operations activities with IA-CND intelligence activities to support intelligence-operations synchronization.
34. Track IAVM/CTO/Warning Order (WARNORD) Compliance.

C.5.4 TASK AREA 4 – ENGINEERING SUPPORT

The Contractor shall provide coverage for all tasks in this Task Area Monday through Friday 0700 to 1800.

C.5.4.1 Project Management

The USCENTCOM J6 provides comprehensive management of IT, telecommunications, and other projects that align with the Command's strategy. The Contractor shall provide assistance in the management of required projects that arise during the period of performance and within scope of the TO. Activities are required to follow the processes, phases, and standards in accordance with project management industry standards. These phases may include, but are not limited to, initiation, planning, execution, monitoring, closing and all applicable processes contained within each phase as they apply to each project. The Contractor shall provide the system engineering deliverables specific to each phase of project management. The Contactor shall track the acquisition and fielding of engineered solutions for HQ USCENTCOM, CFH, and the USCENTCOM AOR. The Contractor shall liaison with USCENTCOM J6 Divisions to provide project coordination and support.

The Contractor's minimal project management goals are:

1. Provide project management using best industry practices such as those provided in the Project Management Institute's Project Management Body of Knowledge (PMBoK).
2. Facilitate the generation of system engineering deliverables within the Initiation Phase – Charter, Information Paper, and Stakeholders documents.
3. Facilitate the generation of system engineering deliverables within the Planning Phase – Requirements document, Project Plan, Test Plan/Results, and Implementation Plan.
4. Facilitate the generation of system engineering deliverables within the Execution Phase – Procurement Documents and Project Brief.
5. Facilitate the generation of system engineering deliverables within the Monitoring Phase – Scope/Pilot Results, Business Rules, and Operational Level Agreement/Memorandum of Agreement.
6. Facilitate the generation of system engineering deliverables within the Closing Phase – Finalized Procurements, Final Project Acceptance, and Lessons Learned documentation.
7. Identify key stakeholders, facilitate the kick-off meeting, and develop the formalized requirements documents for special projects within 15 workdays of project kick-off.
8. Ensure all coordination is performed with Change Management, Configuration Management, and Portfolio Management for special projects within five workdays of project kick-off.
9. Develop project plan, determine milestones, and establish the timeline for special projects within 20 workdays of project kick-off.
10. Coordinate with project stakeholders and comply with policy and with strategic objectives, policies, and portfolio plans for special projects.
11. Coordinate with Division and Branch Chiefs on specific project requirements for clarity of scope of projects.
12. Perform Risk Management throughout the project life cycle for special projects - identify/analyze/mitigate, accept, or ignore.
13. Consolidate USCENTCOM requirements to minimize redundant projects and ensure that they are technically relevant to the mission of the command.
14. Maintain project schedules, templates, and reports through the use and collaboration of MS Project, MS Office Products, and MS SharePoint automated tools.

15. Coordinate with CCJ6-C (Cyber Division) for all IA accreditation requirements for all projects.
16. Coordinate with CCJ6-P (Programs and Architectures Support Division) for all portfolio management requirements to include, but not limited to, eQuad, Form 3215, and USCENTCOM Regulation (CCR) 25-200 compliance.
17. Coordinate with USCENTCOM CCJ6-R (Resources and Analysis Division) to provide procurement documentation: Bill of Material, Statement of Work (SOW), Vendor Quotes, Brand Name Justification, and Sole Source Justification.
18. Coordinate with Change/Configuration management for the Technical Assessment Process/Configuration Control to include, but not limited to: Preliminary Service Design Review Board, Production Readiness Review Board, Operational Readiness Review Board, Post-Implementation Review Board, and Information Systems Requirements Board.
19. Track the fielding/installation of procured hardware/software solutions.
20. Prepare and maintain Action Officer-level project status brief of all projects currently managing.
21. Attend Division-level meetings as scheduled by Division or Deputy Chief to provide project management input.
22. Participate as SMEs at major national and international technical meetings as identified by USCENTCOM.

C.5.4.2 Engineering Support

C.5.4.2.1 Engineering and Technology Support

The role of the CCJ6 Engineering Division (J6-E) is that of the primary interpreter of operational technologies, issues, and decisions. The J6-E office is responsible for monitoring, assessing, and evaluating technology, and recommending appropriate technology solutions to support the policies and directives issued by the CIO and in support of USCENTCOM J6 strategic plans and initiatives.

USCENTCOM specifically requires systems engineering and technical integration support for technology insertions in support of the USCENTCOM mission. Current technical integration efforts are focused on, but not limited to: Public Key Infrastructure (PKI), CENTRIXS, Active Directory, mobile hand-held devices, and VOIP.

The Contractor shall:

1. Provide guidance as SMEs shaping the USCENTCOM C4 technical posture.
2. Provide technical integration tasks to include testing and evaluating system architectures/engineering design.
3. Recommend technical solutions to system shortfalls, emerging technologies, or proposed projects.

4. Perform technical system configuration and administration in accordance with industry best practices, system documentation, and the Program Management Plan.
5. Develop administrator training materials and deliver administrative training. Maintain technical systems documentation, test results, and administrator training materials.
6. Test and evaluate system architectures and engineering design.
7. Coordinate, develop, and evaluate technology support, infrastructure operations, Commercial Off-The-Shelf (COTS)/Government Off-The-Shelf (GOTS) systems, custom applications, IA, and standards needed to provide flexible and effective IT services and capabilities.
8. Provide technical guidance for the development of Information Resource Management (IRM) strategy and policies.
9. Evaluate new technologies in accordance with the CCR 25-200 process.
10. Research and propose solutions to enable the modernization of the USCENTCOM IT architecture and integrate new technologies. Monitor emerging technologies and industry best practices and provide recommendation for IT refresh opportunities.
11. Research, review, analyze, and provide technology solutions to ensure the security and protection of USCENTCOM's information resources.
12. Identify and recommend business process improvements through the application of technology.
13. Provide operational oversight and priority guidance for all technology related TO efforts.
14. Plan, coordinate and establish near-term and long-range goals and objectives that provide the foundation for C4 technical products, services, and methodologies and ensure these are written into appropriate contracts, Service Level Agreements (SLAs), etc.
15. Gather technology requirements from J6 Directorate for evaluation, acquisition recommendation, and implementation.
16. Support the Configuration Control Board (CCB).
17. Coordinate, review, analyze, and draft responses regarding DoD, Office of the Secretary of Defense (OSD), JS, USCENTCOM, and Directorate tasks IAW USCENTCOM staffing procedures and guidance.
18. Assist in the planning process to integrate new systems in the theater architecture.

The contractor shall provide Tier 3 and Tier 4 support as necessary to support the USCENTCOM IT Infrastructure. Tier 3 support shall be classified as expert (advanced) level support to solve complex problems which adversely impacts the enterprise. In addition, Tier 3 support will encompass any issue which cannot be resolved at the Tier 2 level at the agreed upon amount of time. Tier 4 shall be classified as immediate support from an outside (external) resource to assist Tier 3 Engineers in resolving crisis situations which cannot be resolved within the agreed up amount of time.

C.5.4.2.2 Engineering Design Analysis

The Contractor shall provide Engineering Design and Architecture support and shall be responsible for providing enterprise engineering support and expertise for voice, data, and

transmissions networks in the USCENTCOM AOR. The Contractor shall develop engineering solutions and COAs to assist forward Components with the integration of new C4 technology in theater. The Contractor shall be responsible for Level III troubleshooting of the voice, data, and transmissions networks in theater and evaluates the effect of architectural changes on the TIG.

The Contractor shall:

1. Provide planning and engineering guidance to component network planners at engineering conferences.
2. Perform C4 network planning for contingencies, exercises, and current operations.
3. Provide detailed planning of C4 network changes to support emerging theater C4 requirements.
4. Review existing, edit, publish, and maintain documentation (written and graphical) of all engineering and design activities of the USCENTCOM C4 theater network in agreed upon and accepted industry standard format.
5. Review, edit, and maintain theater C4 network roadmap and required network changes for next 120 calendar days.
6. Identify and recommend tools and processes to accomplish CCJ6 enterprise management (NetOps) tasks.
7. Identify theater requirements for strategic assets (e.g., strategic satellite terminals, strategic voice switches, strategic multiplexers, and strategic data routers).
8. Identify re-utilization/re-allocation of strategic theater assets based on requirements.
9. Provide design/architectural recommendations for long-term/chronic problem resolution.
10. Provide Level III engineering assistance for immediate and emergency troubleshooting and problem resolution.
11. Maintain proficiency in current industry standards such as American National Standards Institute (ANSI), Institute of Electrical and Electronics Engineers (IEEE), and Bellmore.
12. Support the planning, execution, and after-action phases of current operations, contingency operations, exercises, and joint network upgrades in the USCENTCOM AOR.
13. Perform monitoring and update the circuit actions database.

The Contractor shall provide support for the following specific subtasks:

Data Network Engineering

The Contractor shall be responsible for providing engineering and technical expertise on all data network issues in theater; engineering and managing the Tier 1 data network in theater; interfacing with DISA to coordinate engineering of Tier 1 to Tier 0 interface connections; addressing interoperability issues and requirements; planning, coordinating and managing IP routing to the DISN backbone; and addressing network routing issues.

Transmissions Engineering

The Contractor shall be responsible for providing engineering and technical expertise on all transmissions network issues in theater; engineering and managing the transmissions network in theater (including military and commercial Radio Frequency (RF), SATCOM, and multiplexing systems). The Contractor shall also interface and coordinate with commercial satellite vendors to obtain transmission plans. The Contractor shall maintain situational awareness of capacity availability over the AOR. The Contractor shall validate theater requirements in accordance with applicable directives.

Information Assurance Engineering

The Contractor shall provide IA engineering in support of the CCJ6-C Cyber Support Task Area IA defense in-depth program for USCENTCOM enterprise networks. The Contractor shall provide a complete and thorough risk assessment analysis of all IS to ensure systems maintain the appropriate level of confidentiality, integrity, availability, and accountability based national and DoD security regulations and directives. The Contractor shall provide security and information engineering support to HQ USCENTCOM, the CFH, Components and JTFs DISN, DSN, and CDS Connection Approval Packages.

The Contractor shall:

1. Perform risk/vulnerability assessment for engineered networks and systems.
2. Ensure engineering tasks and solutions comply with USCENTCOM accreditation, certification and connection standards for HQ's and theater's networks and systems.
3. Engineer and analyze solutions for vulnerability and risk assessment to ensure solutions are in compliance with security standards and measures.
4. Coordinate with subordinate, adjacent, supporting, and senior organizations and agencies to support resolution of security issues, accreditation and connection approval, and engineering requests.
5. Engineer solutions that ensure network security accreditation and policy support tasks, including project management support services.
6. Perform review, analysis, and documentation for the life cycle security requirements of applications, systems, and networks within the HQ USCENTCOM.
7. Review Security Test and Evaluation plans; develop or refine if necessary.
8. Advise the Theater IAM, Chief of C4 Plans and Operations, USCENTOM Certification Authority, and the Theater Designated Approval Authority (DAA) of network and system risks, risk mitigation, COAs, and operational recommendations.

Information Systems Engineering

The Contractor shall support the integration and resolution of issues pertaining to Joint Theater Enterprise-wide Application Services and Systems. Enterprise Application Services and Systems consist of networked applications and systems providing critical end-user services. These systems provide web-based services, remote-hosted applications, discovery, storage, software applications, operating systems, and databases.

C.5.4.2.3 Coalition Network Architecture Engineering

The Contractor shall perform Coalition Network Architecture Engineering support to provide network engineering and management support of coalition networks in theater. The Contractor shall be responsible for evaluating new requests for service and providing engineering solutions in the form of COAs. Additionally, the Contractor shall be responsible for interacting with Components and other Directorates to ensure proper engineering of systems supporting Coalition Communications.

The Contractor shall provide engineering and technical expertise on all coalition data network issues in theater. The Contractor shall engineer and manage the Tier 1 coalition data network in theater. Additionally, the Contractor shall interface with Components and other Directorates to coordinate engineering; address interoperability issues and requirements; plan, coordinate, and manage IP routing to the DISN backbone; and address network routing problems. The Contractor shall also coordinate and provide network troubleshooting guidance to forward units; identify, diagnose, and resolve complex problems affecting coalition network performance; provide planning and engineering guidance to component coalition network planners at engineering conferences; and develop and maintain coalition data network SOPs and TTPs for the theater

The Contractor shall:

1. Assist in C4 network planning for contingencies, exercises, and current operations.
2. Recommend tools and processes to accomplish CCJ6 enterprise management tasks.
3. Review and validate Component and Coalition Joint Task Force (CJTF) C4 network plans and network changes.
4. Identify theater requirements for strategic assets (e.g., strategic satellite terminals, strategic voice switches, strategic multiplexers, and strategic data routers).
5. Identify re-utilization/re-allocation of strategic theater assets based on requirements (i.e., re-allocate satellite terminals, voice switches, etc.).
6. Provide Level III engineering assistance for immediate and emergency troubleshooting / problem resolution.

C.5.4.2.4 Configuration and Enterprise License Management

USCENTCOM is responsible for multiple networks, including U.S.-only classified and unclassified, as well as Coalition and bilateral networks, connected to countries in the AOR. The Contractor shall establish and operate a Configuration Management program on all networks at HQ, CFH, and TNC. Configuration items required to deliver IT services are managed and maintained in accordance with IT Service Management (ITSM) practices. The Contractor shall support hardware and software re-capitalization planning, managing the command approved software and hardware lists and its associated documentation library. Tasks shall also include providing technical inputs to policies and procedures, The Contractor shall develop configuration management utilities and recommend the use, operation, and maintenance of software and applications to support configuration

management, asset management, release management, and license management for all applications and systems.

The Contractor shall operate a software inventory management program to ensure compliance with DoD policy and other Federal laws and ITSM best practices. The Contractor shall monitor, track, and ensure that the software in use on all USCENTCOM networks has licenses and maintenance agreements. The Contractor shall research licensing alternatives and present the best licensing alternatives to USCENTCOM. The Contractor shall consider usage trends, migration plans, operational changes, and return on investment (ROI) when researching alternatives. The Contractor's program shall maximize ROI and maintain the warranty and maintenance coverage for all hardware and software (including Contractor-purchased items and Government-purchased items).

The Contractor is required to maintain and control all versions of existing Configuration Items (CIs) used in the provision and management of its IT services at USCENTCOM. The Contractor shall perform and provide configuration management that is accurate and up-to-date by managing the life cycle of all CIs from acquisition to termination.

The Contractor shall:

1. Provide asset management with a CMDB to implement a hardware maintenance/warranty program to monitor and track assets.
2. Analyze and support CCJ6 management on the development of configuration management policies and procedures for CCJ6 approval and implementation.
3. Review existing and edit and maintain configuration management utilities to automate software and applications for configuration management, asset management, and license management.
4. Update and maintain configuration management policy documents upon CCJ6 approval.
5. Maintain the Command-approved hardware/software list for all authorized software and hardware at HQ and CFH.
6. Track licenses, maintenance plans, and renewal information for all software on the approved software list.
7. Coordinate with appropriate USCENTCOM staff when users request upgrades to existing applications, and maintain configuration documentation.
8. Implement and maintain a CMDB that contains details of the CIs throughout their life cycle and that provides accurate information to support all the other service management processes.
9. Perform scheduled audits against the CMDB to verify the data remains current and accurate (CMDB Reconciliation).
10. Create tools/reports to help gather Key Performance Indicator (KPI) information to be used to better processes and procedures and aid leadership in making informed decisions.
11. Establish and maintain the Definitive Software Library (DSL) and Definitive Hardware Library (DHL) stored in the CMDB.

12. Perform reviews that assert that CIs actually exist, and check that these CIs are correctly detailed in the CMDB.
13. Provide recommendations for changes to the CIs to include suggestions for new procedures, additional skill sets, technology refreshment, modified configurations, etc.
14. Develop and implement a plan to replace key IT assets and CIs at regular intervals throughout their life cycle.
15. Maintain and control legal documents (software contracts and renewals) in the Configuration Management System
16. Develop and control a naming convention process for all hardware on the operational networks; perform records management function IAW DoD policies.
17. Develop and maintain regulations, TTP, and SOP documentation of procedures and processes of how duties are performed.
18. Keep documentation and work status current.
19. Provide technical assistance to ensure all Automated Data Processing (ADP) hardware purchased by USCENTCOM is in compliance with the most current approved "Standard Configuration."

C.5.4.2.5 Engineering Monitoring Tools Support

The Contractor shall maintain USCENTCOM Engineering monitoring toolset. The Contractor shall be responsible for deploying toolsets to strategic locations in the AOR to ensure comprehensive network view of the TIG from Tier 0 to Tier 2, and configuring systems to enable communications among components.

The Contractor shall:

1. Design, construct, test, and implement an integrated monitoring environment for network hardware and software solutions, distributed computing solutions, and physical/logical communications networks.
2. Plan, implement, and support existing network management systems employed in USCENTCOM AOR.
3. Implement monitoring systems to meet information exchange requirements.
4. Analyze and provide recommendations of management system and product integration, implementation, and deployment in support of enterprise-wide strategies for provisioning, operations, monitoring, and maintenance.
5. Analyze and develop management architecture concepts, alternatives, and strategies.
6. Develop and implement prototypes, proof-of-concept demonstrations, and hands-on engineering of management solutions.
7. Analyze and provide recommendations for the tailoring and use of operational process models based on accepted industry standards such as IT Infrastructure Library (ITIL) and Tivoli Management Framework (TMF).
8. Configure monitoring and reporting tools, create custom scripts as necessary, and ensure Components have correct configurations to enable monitoring.

9. Audit tool configurations and hardware/software inventories to validate comprehensive monitoring.
10. Integrate several network monitoring/management tools into comprehensive view.
11. Perform daily operations and maintenance of servers running MS Windows Server NT, 2000, 2003, 2008, and XP and UNIX Operating Systems.
12. Troubleshoot issues with existing or developed systems and work with the appropriate resources to resolve them.
13. Provide technical systems support to deployed forces.
14. Develop, implement, and maintain MS Standard Query Language (SQL), MySQL, Oracle, UNIX-based, and LINUX-based databases to support Command requirements. Troubleshoot issues with existing or developed systems and work with the appropriate resources to resolve them.
15. Maintain currency on the following code used for development: SQL, Active Server Page (ASP), .NET, Visual Basic (VB), HTML5, and JAVA scripts.
16. Write Stored Procedures and Triggers as needed in database development.
17. Develop database interfaces to Command and Directorate/Agency databases.
18. Operate, maintain, and administer database servers, hardware, and software.
19. Develop and document system administration, database management, and user guidance on use and management of databases and provide input to database policy guidance for the Command.
20. Develop graphics and layouts for product illustrations, architectural diagrams, and internet websites.
21. Maintain central repository of diagrams and distribute via on-line portal.
22. Determine size and arrangement of illustrative material and copy.
23. Prepare illustrations or rough sketches of material to support network engineering branch.
24. Creates graphics artwork to support projects, programs, and presentations.
25. Maintain currency on IEEE Professional Communications Standards.
26. Develop, write, and edit material for reports, manuals, briefs, proposals, and related technical and administrative publications.
27. Ensure currency of USCENTCOM CCJ6 official publications (i.e., 25-206, SOPs, TTPs).
28. Develop studies, blueprints, sketches, drawings, part lists, and specifications.
29. Create and maintain theater engineering documentation (Tier 1 voice, data, transmissions architectural diagrams) using MS VISIO, AutoCAD or other approved drawing package.
30. Develop diagrams and drawings to support engineering projects.
31. Research and document theater data flows (high-level and detailed).
32. Extract information from various sources (i.e., current diagrams, configuration, files, etc.) to create architectural diagrams.
33. Compose instructions, policies, and procedures related to USCENTCOM theater engineering and C4 network operations.
34. Develop and maintain Concepts of Operations and regulations.

The Contractor shall provide support for the following specific subtasks:

System Administration
The Contractor shall providing daily technical server and computer maintenance, providing systems support to deployed forces, trouble-shooting and reconfiguring systems; daily operations and maintenance of servers running MS Windows Server NT, 2000, 2003, 2008, and XP and UNIX operating systems; troubleshoot issues with existing or developed systems and work with the appropriate resources to resolve them; developing and documenting system administrator and user guidance on operations and management of systems and provide input to system administrator policy guidance for the Command; and ensuring reliability of C4 systems.

Database Administration
The Contractor shall operate, maintain, and administer database servers, hardware, and software in support of network management platforms; provide technical problem solving for customer computer support of database applications; develop, implement, and maintain MS SQL, MySQL, Oracle, UNIX-based, and LINUX-based databases using code for development which includes SQL, ASP, .NET, VB, and JAVA scripts; troubleshoot issues with existing or developed systems; work with the appropriate resources to resolve them; and develop database interfaces to Command and Directorate/Agency databases.

Remedy Administration
The Contractor shall perform daily operations and maintenance of servers running Remedy Applications, provide systems support to deployed forces, develop and document system administrator and user guidance and provide input to system administrator policy guidance for the Command.

C.5.4.2.6 Change Management

The Contractor shall standardize methods, processes, and procedures to control and improve the quality of the day-to-day operational IT support.

The Contractor shall:

1. Align the IT services to actual business requirements.
2. Increase visibility and communication of changes to customers and support staff.
3. Reduce negative impacts of changes on the networks.
4. Improve risk assessments to determine operational and technical impact.
5. Reduce disruptions and improve productivity and quality of services while decreasing re-works.
6. Improve the ability to handle a greater volume of changes.
7. Identify and record changes.
8. Assess the impact, benefit, and risk of proposed changes.
9. Present a business case for proposed changes.

10. Manage, coordinate, and implement changes.
11. Monitor and report change implementations.
12. Review and close requests for change (RFCs).
13. Facilitate and administer the Change Advisory Control Board (CAB).
14. Identify and recommend tools and processes to accomplish CCJ6 enterprise management tasks.

C.5.4.3 Test, Analysis, and Integration Lab Support

The USCENTCOM Test, Analysis, and Integration Lab is responsible for testing, analyzing, and integrating into production the technical solutions that meet USCENTCOM strategies. In addition, the Contractor shall provide solutions to unique production network and mobile communication issues. USCENTCOM's lab supports all the Command's unclassified, secret, and coalition networks at HQ, CFH, and TNC, as well as mobile products. USCENTCOM must develop and integrate systems to support day-to-day garrison operations, as well as develop and maintain robust and survivable C4 systems.

The Contractor shall test all hardware, software, and network configuration upgrades, additions, or revisions in the laboratory for Government approval before implementation. This includes downward-directed systems underwritten by the JS or other Government agencies. The CCJ6 also relies on laboratory testing and recommendations before approving any hardware or software additions or upgrades to the Command networks. The Contractor shall also perform, as directed, comparison testing and associated test reports (Decision Analysis Report) of similar products in order to determine which product(s) is/are most well suited to fulfill Central Command requirements.

The Contractor shall:

1. Provide information testing, analysis, and integration, as well as associated written reports, for USCENTCOM strategies.
2. Perform broad network, computer, and mobile engineering tasks.
3. Apply expertise on multiple aspects of computer network architectures on complex, cross-connected systems. Network expertise includes operational processes, hardware, software, and security.
4. Perform network, computer, and mobile engineering research, design, and testing.
5. Perform in-depth analysis of complicated systems to determine which are capable of supporting functional requirements and should continue to be used, which should be enhanced, and which should be replaced by more advanced designs.
6. Perform architectural planning, integration and compliance testing of all hardware and software proposed for deployment within the USCENTCOM enterprise.
7. Create quarterly command standard baseline load set for all clients (thick and thin clients and Virtual Desktop Infrastructure (VDI)).

8. Perform information security and information assurance assessments and recommendations to include IAVA and IAVM applicability assessments and integration testing.
9. Provide Tier III/IV support to CCJ6-SO for both workstation and network issues.
10. Build and maintain a variety of test bed environments. For example: NIPRnet, SIPRnet, CENTRIXS and others that may be needed in order to evaluate and demonstrate new technologies.
11. Develop virtual packages for approved software that are required to be delivered to user workstations.
12. Evaluate and respond to Change Requests, Problem Tickets and Incidents, as required.

C.5.4.4 Software Engineering Support

USCENTCOM is required to develop/integrate network web systems and databases, which can provide support of day-to-day garrison operations. USCENTCOM CCJ6 provides direct technical support, ADP testing, and systems integration and application development and maintenance in support of USCENTCOM Command and Control, Communications and Computers Systems and Intelligence (C4) initiatives. The USCENTCOM Software Engineering Support Branch program develops and integrates systems to support day-to-day Government garrison operations, as well as transitions quickly to reliable wartime support for the CFH. Web/portal pages, databases, applications, and interfaces reside on SIPRNet, NIPRNet, and CENTRIXS networks. It is necessary to ensure that the Command Software Engineering Branch possess the expertise to maintain web/portal capabilities and applications and develop and maintain databases. The code used for development includes C, SQL, ASP, .NET, VB, and JAVA scripts.

The Contractor shall:

1. Provide engineering support with both locally developed software and COTS software in the Command.
2. Provide systems integration, testing, maintenance, installation, configuration, and troubleshooting for all databases and web/portal applications.
3. Provide SharePoint, including architecture, installation, configuration, and best practices.
4. Serve as technical database systems developer for the Command's SQL databases and multiple SQL servers and technical expert on all web servers.
5. Assist with monitoring operation of databases/web servers and ensures software and hardware are functioning properly and operational standards are met.
6. Provide technical guidance on the implementation of new web, database, and portal software.
7. Implement security and access controls requested by content providers and page maintainers.
8. Work with USCENTCOM SMEs to capture business processes through customer interviews and finalizing requirements gathering.
9. Assist with development of software design documents (SDD) for creation of knowledge management functions within the portal environment.

10. Ensure architecture data integrity and consistent integration and conformity of products to the DoD standards. Support gathering, documenting, testing, deploying, and marketing of web content to support business processes within USCENTCOM.
11. Support web/database development and administration on the SIPRNet, NIPRNet, and coalition/allied networks throughout the AOR. The Contractor shall be responsible for all SQL databases and web applications/pages.
12. Provide technical support based on web policies stated in OSD Web Site Administration, DoD Instruction 5230.29, and DoD Directives 5230.9 and 5200.40.
13. Convert and develop SQL databases to support Command's requirements.
14. Develop, test, and implement web parts for the portal.
15. Provide policy and procedures for training users on new web/database applications.
16. Troubleshoot issues with existing or developed systems and work with the appropriate resources to resolve them.
17. Understand and develop reports using SQL Reporting Tool.
18. Write Stored Procedures and Triggers to incorporate them in the database development.
19. Develop, maintain, and administer Command-level web pages on the USCENTCOM Intranet (CENTRANET), SIPRNet, NIPRNet, and Coalition/Allied networks for garrison and deployed. Identify, recommend, develop, and implement web tools and applications.
20. Coordinate/assist Directorate/Agency webmasters in developing web/portal pages.
21. Integrate Directorate/Agency web/portal pages with Command-level pages.
22. Develop web interfaces to Command and Directorate/Agency databases and files. Identify, recommend, develop, and implement solutions to customer requirements for greater availability to data and services hosted on web.
23. Operate, maintain, and administer web and portal servers, hardware, and software.
24. Coordinate with network system administrators to minimize network service disruption.
25. Develop and document web management and user guidance on use and management of web pages and provide input to web policy guidance for the Command.
26. Provide ongoing support, resolution of problems, and recovery of operational malfunctions involving hardware/software failure.
27. Coordinate with security personnel and ensure latest IAVAs are loaded within the designated timeframe.
28. Identify and assign (with Government approval) permissions and roles to databases.
29. Analyze database design and structure and recommend changes to improve performance.
30. Provide training to functional area database administrators.
31. Document all upgrades to hardware and software within three workdays of upgrades.
32. Keep database server information current in database. Information shall be updated within two workdays after new servers have been put online or old servers are retired.
33. Meet with users and assist system analysts with creation of requirements packages.
34. Complete a comprehensive, multi-disciplinary security assessment addressing both content and technical issues at least annually on all web servers.

35. Update incidents, work orders, and change requests at a minimum of every five workdays.
36. Notify Customers within ten workdays after submitting a request for new software.
37. Update information in the portal and develop a project plan and briefing if customer requests need major development not later than five workdays after first customer meeting.
38. Develop mobile applications to support the Command.
39. Design, develop, maintain, and enhance applications software for the Combatant Command Joint Operations Center (JOC) responsible for maintaining situational awareness and joint operations across the Area of Responsibility at the four-star Command level.
40. Consult with and advises managers and functional users in an effort to develop unique requirements necessary to meet their Information Technology (IT) demands.
41. Perform in-depth analysis of complicated systems to determine which are capable of supporting functional requirements and should continue to be used, which should be enhanced, and which should be replaced by more advanced designs.
42. Support the development of Common User Interface in order to achieve a Common Operating Picture (COP) across the Theater.

C.5.5 TASK AREA 5 – CYBER SECURITY

The Contractor shall provide the following support for all of the tasks/subtasks under this Task Area:

1. Develop and provide threat briefs to USCENTCOM leadership.
2. Maintain an in-depth understanding and uphold DoD and USCENTCOM policies, regulations, and guidelines as it relates to Information Assurance and Computer Network Defense; assisting customers and responding to requests for information in a timely manner (not to exceed 48 hours).
3. Prepare and provide threat and/or risk briefings to USCENTCOM leadership.
4. Analyze trends and publish summary reports on a monthly basis where applicable within the task order
5. Maintain and develop detailed operational checklists to ensure all personnel follow standard operating procedures; ensuring all personnel are properly training on performing daily operational tasks.
6. Provide subject matter expertise required to respond to Joint Staff Taskers.
7. Maintain a continuity folder of documentation pertaining to all systems and technologies that are relevant to this task area in order to facilitate training. As new systems and technologies are introduced, develop and maintain additional information required.
8. Develop and publish best practices, policies, and procedures for IA/CND within the scope of each specified task.

C.5.5.1 Headquarters Network Defense

Description:

The Contractor shall protect and defend the IT infrastructure located at HQ USCENTCOM and CFH. The Information Assurance (IA)/Computer Network Defense (CND) program shall support Command security policy, plans, exercises, and incident handling and response.

The Contractor shall:

1. Provide dedicated, on-site support for all cyber security operations within the scope of this task.
2. Operate and maintain network defense systems within the scope of this task to include disaster recovery and contingency planning.
3. Ensure adequate measures and mitigation strategies are in place to properly detect and defend the HQ locations and extensions.
4. Analyze and isolate security intrusions, security incidents/compromises, and malware for all servers, clients, and other infrastructure within the scope of this task. Publish a report summarizing all findings on a daily basis; provide a trending report on a monthly basis.
5. Analyze security events reported by routers, firewalls, and Intrusion Detection System (IDS) sensors within the scope of this task. Publish a report summarizing all findings on a weekly basis.
6. Develop system policies and signatures to detect, prevent, and report intrusions.
7. Perform trend analyses of security events. Based on these analyses, identify areas that need improvement and recommend security controls and best practices that should be implemented to mitigate any security problems and vulnerabilities detected.
8. Assist with the maintenance of accreditation documentation for all systems and networks within the scope of this task IAW DIACAP.
9. Perform network and system security reviews (reportable under Federal Information Security Management Act (FISMA)) to include CTO and routine vulnerability scanning of HQ networks.
10. Perform network and system security audits IAW USCENTCOM policies, regulations, to detect malware and unauthorized access to USCENTCOM networks.
11. Develop and maintain a database of known malware signatures to enable the detection of malware during network scans.
12. Perform forensics collection on all networks within the scope of this task.
13. Maintain a program to monitor portable electronic devices within the perimeter.
14. Conduct active cyber defense response operations by leveraging host, network, dynamic data acquisition, and intelligence in order to identify, characterize, and counter adversarial cyber threats.
15. Utilize knowledge of packet analysis and network trending to establish a baseline of network traffic and determine if there are any anomalies within the traffic.
16. Collect, process, and/or fuse information from all authorized cyber threat intelligence reports and outside agencies in support of indications and warning development to identify and attribute anomalous/nefarious network activities.

C.5.5.2 Theater Cyber Initiatives

Description:
The Contractor shall provide security management support for IA and Strategic Enterprise Computer Network Initiatives. The objective of these tasks is to support USCENTCOM's efforts to direct and synchronize IA/CND actions and activities to proactively defend the USCENTCOM portion of the GIG, as well as to provide theater network security situational awareness to the USCENTCOM Commander.

The Contractor shall fuse IA/CND threat information and other information sources to provide predictive warning, threat analysis, and course of action recommendations to support current and long-term network defense mitigation strategies, as well as collaboration with the information operations community of interest.

Activities:

The Contractor shall:

1. Provide dedicated, on-site coverage for all systems/services operated and maintained by the Theater Cyber Initiatives Support Team. On-call support shall be provided during non-duty hours. The maximum time for reporting to duty station after on-call support is requested is one hour from the time of notification. A comprehensive on-call/alert roster shall be maintained and updated on a monthly basis.
2. Assess capabilities and gaps in theater network security surveillance; document recommended changes to sensors based on cyberspace indications and warnings.
3. Publish cyber security trend analyses of theater assessments, lessons learned, and recommended mitigation approaches within 30 calendar days of the completion of an assessment.

The Contractor shall provide support for the following specific sub-tasks:

Theater Cyber Infrastructure Programs Sub-Task Activities:
Manage the production of cyberspace threat reports and products that support situational awareness, planning, operations, and response actions including, but not limited to, the following:

1. Contribute to cyber-related tasks, initiatives, and the development of long range strategies.
2. Provide subject matter expertise to assist with course of action development and implementation of an enduring IA enterprise mitigation strategy.
3. Draft and coordinate CTOs or other directives that affect network configuration, change the information operations condition, or influence operational changes based on cyberspace threat warnings, vulnerabilities, or chronic cyber-related issues that plague the warfighter.

4. Manage and respond to RFIs from USCENTCOM components, IA/CND sections, and NetOps decision makers in order to support theater program initiatives.
5. Improve theater security posture by managing, tracking, and providing situational awareness for all USCENTCOM-directed strategic theater programs.
6. Provide IA/CND subject matter expertise to support planning, current operations, and security engineering activities.
7. Recommend technology upgrades and modifications based on evolving technologies, best practices, and strategic initiatives.
8. Provide current cyberspace threat information through analysis and fusion of relevant information.
9. Develop, perform, and manage a theater cyberspace threat information collection plan through RFIs and support from various internal/external organizations and agencies.

Theater Cyber Training and Awareness Sub-Task Activities:

1. Develop and maintain an effective and relevant security training and awareness program that follows Federal, DoD, and USCENTCOM policies, regulations, and standards.
2. Develop, implement, and help enforce relevant cyber security training for HQ USCENTCOM and its theater components.
3. Develop training requirements for cyber-related threats based on mission and situational needs.
4. Facilitate/coordinate metrics and trend to identify common security digital signage platform and all other means of message conveyance.
5. Draft policy guidance resulting from C4SR Operational Planning Team (OPT) conferences, Relieve in Place (RIP)/Transfer of Authority (TOA) events, and exercise planning conferences.
6. Assist USCENTCOM in the planning and execution of the Theater Cyber Training Program.

Theater Cyber Assessments Sub-Task Activities:

1. Assess annually the security posture at each USCENTCOM theater Component HQ and ensure their compliance with all DoD and USCENTCOM guidance. Publish an assessment schedule and create a report summarizing all findings and mitigation actions taken within 60 calendar days of the completion of each assessment.
2. Provide theater IA/CND situational awareness through well-coordinated assessments of all components to measure their IA readiness.
3. Perform analyses of findings; develop metrics and trends to identify common theater security weaknesses.

Theater Cyber Defensive Policy Sub-Task Activities

1. Assist with the collection of cyberspace threat information from the following sources:

- Law enforcement community products, databases, websites, and tools.
- Commercial/open source products, databases, websites, and tools.
- Locally generated databases, websites, and tools.
- Other relevant sources of information.

2. Manage cyber-related information to provide ready access for rapid correlation, analysis, and dissemination.
3. Recommend changes to USCENTCOM network surveillance resources based on cyberspace indications and warnings.
4. Assist USCENTCOM with collaborative theater IA/CND planning and operations utilizing email, chat, and other online collaboration technologies.
5. Disseminate cyberspace information to decision makers, as well as the IA/CND, NetOps, and information operations communities to support planning, operations, and other related activities.
6. Produce and track the status of all Cyber CTOs, fragmentary orders, Network Defense actions, and record messages.

C.5.5.3 Cyber Certification and Accreditation

Description:
The Contractor shall provide certification and accreditation assistance in support of the IA defense in depth program for USCENTCOM enterprise networks. This shall include a complete and thorough risk assessment of all information systems to ensure that these systems maintain the appropriate level of confidentiality, integrity, availability, and accountability based national and DoD security regulations and directives. A central part of this risk assessment is the processing of Connection Approval Packages for the DISN, the DSN, and CDS submitted by HQ USCENTCOM, Service Components, and JTFs.

The Contractor shall:

1. Provide dedicated, on-site coverage for all systems/services operated and maintained by the Theater Certification and Accreditation Support Team. On-call support shall be provided during non-duty hours. The maximum time for reporting to duty station after on-call support is requested is one hour from the time of notification. A comprehensive on-call/alert roster shall be maintained and updated on a monthly basis.
2. Execute the HQ USCENTCOM Certification and Accreditation (C&A) program.
3. Maintain, track, and validate DISN, DSN, and CDS Connection Approval Packages for USCENTCOM to include Components and JTFs.
4. Perform risk/vulnerability assessments of HQ networks and systems; prepare a risk assessment report for submission to the CA and DAA.
5. Help enforce accreditation, certification, and connection standards for HQ's and Theater's networks and systems.
6. Provide C&A training and briefs to USCENTCOM and its Theater elements.
7. Perform C&A evaluations on new and existing Theater systems and networks for the USCENTCOM Chief Information Officer (CIO) in support of the CCR 25-200 process.

The Contractor shall provide support for the following specific sub-tasks:

Headquarters Certification and Accreditations Sub-Task Activities:

1. Track and maintain certification information databases, websites and tools to ensure that USCENTCOM networks, systems and devices are properly documented and managed from a security perspective. These include but are not limited to:
    - Government Interconnection Approval Process (GIAP) database
    - Standard Network Access Protocol (SNAP) database
    - Ports, Protocols, and Services Management (PPSM)
    - DoD IT Portfolio Repository
    - DoD IT SIPRNet Registry
    - Enterprise Mission Assurance Support Service (eMASS)
    - FISMA
    - Local databases, sites, and systems.
2. Ensure timely notifications are made to prevent lapses in accreditations (i.e., 30/60/90 day notices).
3. Perform vulnerability and risk assessment on IS to ensure they are in compliance with security standards and measures.
4. Coordinate with subordinate, adjacent, supporting, and senior organizations and agencies to support the resolution of security issues, accreditation and connection approvals, and waiver requests.
5. Perform network security accreditation and policy support tasks, including project management support services.
6. Perform review, analysis, and documentation for the life cycle security requirements of applications, systems, and networks within HQ USCENTCOM.
7. Review Security Test and Evaluation Plans; develop Security Test and Evaluation Plans if necessary.
8. Advise the Theater Information Assurance Manager (IAM), Chief of C4 Plans and Operations, and the Theater DAA of network and system risks, risk mitigation courses of action and operational recommendations.
9. Advise the USCENTOM CA and the DAA on network and system risks, risk mitigation, COAs, and operational recommendations.
10. Perform C&A of HQ's systems and networks fielded or supported by USCENTCOM J6 staff IAW DIACAP requirements.
11. Perform risk assessments on systems, applications, and baselines in support of certification.
12. Prepare risk assessment and certification reports and letters.

Theater Connection Approval Support Sub-Task Activities:

1. Execute DISN, DSN, and CDS Command Automation Plan (CAP) program as defined under US Cyber Command (CYBERCOM)/DISA general guidance.

2. Ensure current theater networks and systems maintain certification and authority to operate as they are modified to meet operational requirements.
3. Ensure timely notifications are made to prevent lapses in accreditations (e.g., 30/60/90 day notices).
4. Coordinate and manage resolutions and responses to CYBERCOM Warning Orders; manage DISN CAP authority to connect to minimize USCENTCOM Components on WARNORD.
5. Recommend connection approval, disapproval, or modification based on security risks and vulnerability.
6. Recommend network configuration, policy, training, operational, or other changes/updates based on assessed risks and/or issues.
7. Advise the Theater IAM, Chief of C4 Plans and Operations, and the Theater DAA on network and system risks, risk mitigation, COAs, and operational recommendations.
8. Help coordinate theater collaboration for IA C&A planning and operations utilizing capabilities such as electronic mail, chat, ticketing, and online collaboration sessions.
9. Support C4SR conferences, RIP/TOA events, exercises, and other sources of policy guidance.
10. Serve as an Operational Planning Team Member or coordinating/supporting member for operational and/or planning tasks assigned to the IA C&A Branch; respond to JS and USCENTCOM taskers and RFIs.
11. Perform C&A for Theater systems and networks fielded or supported by USCENTCOM J6 staff IAW DIACAP requirements.
12. Review and support C&A for theater systems and networks fielded or supported by USCENTCOM staff directorates, Components, and JTFs.
13. Serve as an IA POC for promotional, test, new, replacement, and/or Contractor equipment being brought under the purview of USCENTCOM-type accreditation.

Theater Cross Domain Interoperability Sub-Task Activities:

1. Ensure current CDS systems operate on USCENTCOM networks IAW applicable regulations.
2. Ensure current CDS systems maintain certification and authority to operate as they are modified to meet operational requirements.
3. Provide IA/DIACAP subject matter expertise to support the evaluation of current and emerging guard and CDS techniques, technologies, and vulnerabilities. Publish a report documenting this information.
4. Provide technical advice/recommendations for meeting new CDS requirements. Publish a report documenting this information.
5. Attend DISN Security Accreditation Working Group or Flag Panel meetings to advocate USCENTCOM, Component, or JTF requirements.
6. Provide situational awareness of CDS systems in the USCENTCOM AOR, including location, capability, network topology/diagrams, missions supported, and other related information. Publish a report that documents this information on a monthly basis.

7. Manage and track requests/requirements for CDS systems supported within the USCENTCOM AOR; staff packages for prioritization and approval to the appropriate authorities; provide Phase tracking and management.
8. Assist USCENTCOM and Components/JTFs in meeting documentation/ processing requirements to support CDS system requests.
9. Support NetOps conferences, RIP/TOA events, exercises, and other sources of policy guidance.
10. Coordinate with USCENTCOM Directorates and Components to ensure that they have the proper accreditation, Secret and Below Interoperability (SABI), and connection approval documentation.
11. Utilize common criteria, SABI, DoD security accreditation, and DISA network connection approval security processes for computer systems and networks. Support security design, testing, and implementation requirements of integrated networks including hardware, software, and port facilities.
12. Ensure timely notifications are made to customers to prevent lapses in the CDS accreditations Defense System Acquisition Working Group (DSWAG) approval process (e.g., Phases I – IV).

C.5.6 TASK AREA 6 – PROGRAMS AND ARCHITECTURES SUPPORT

C.5.6.1 Programs and Architectures

C.5.6.1.1 Program Planning and Development Support

The Contractor shall provide support to implement a program to properly integrate new systems into USCENTCOM and aid in coordination of actions across the AOR. USCENTCOM also needs to have more visibility into Life Cycle Management issues for maintaining existing systems and fielding new IT systems. The Contractor shall coordinate, plan, and integrate IT systems in the procurement process, and shall focus on matching requirements (capability) with resources (finances) for the short-term and creating a more cohesive long-term plan to serve both the Command and AOR elements.

The Contractor shall:

1. Advise the CIO regarding a net-centric enterprise approach to IRM and IT application within the command.
2. Support the J6 strategies in meeting the mission in providing net-centric solutions for the warfighter.
3. Coordinate, develop, and evaluate governing policies needed to provide flexible and effective IT services and capabilities.
4. Implement the J6 IRM strategy.
5. Ensure strategic plan is supported by the latest in proven advanced technology by monitoring, assessing, and evaluating emerging technological solutions.

6. Analyze integration effort to ensure compatibility and functional performance compliance to the requirements in consideration future projects or upgrades. Identify projected shortfalls and recommended corresponding solutions.
7. Develop and execute operational tests to the systems to ensure compatibility and functional performance.
8. Perform business process analysis, develop requirements definition, and produce program documentation.
9. Develop a comprehensive transition plan for the program.
10. Develop comprehensive strategic engagement plans to shape Service- and DoD-level programs in support of USCENTCOM's mission requirements.
11. Draft USCENTCOM Theater policy and guidance to govern the use of program area applications, systems, and IT capabilities.
12. Develop, submit, and synchronize all Program Objective Memorandum (POM) data with the military services for all program area systems, applications, and IT capabilities within the USCENTCOM Theater to ensure continuity of capability across the Theater.
13. Research and develop initial Project Management Charters (PMC), kick-off briefings, and project scope statements.
14. Synchronize Joint/DoD, and Service-level technology insertions via a network of HQ, Service component, and JTF project managers to achieve continuity of capability within the AOR.
15. Produce decision and information briefings/papers and status frameworks for all applicable programs, projects or processes.
16. Develop project plans for technology insertion projects.
17. Develop project-level resource and procurement strategies via a financial plan to execute technology insertion projects.
18. Develop management structures to ensure all manpower and support relationships are well-defined to support implementation and transition to operations and maintenance.
19. Perform detailed systems analysis and design for development of operational/functional, systems, and technical architectures.
20. Develop, coordinate for, or review detailed C&A documentation in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) or emerging DIACAP process.
21. Analyze risks and develop accompanying mitigation plans to support Theater-wide technology insertions.
22. Develop Quality Assurance and Testing Plans to ensure interoperability with current USCENTCOM C4 baseline.
23. Coordinate and synchronize technology insertion efforts with the JS, DISA, Military Services (U.S. Army (USA), U.S. Air Force (USAF), U.S. Navy (USN), and U.S. Marine Corps (USMC)) and subordinate service components and JTFs in Theater.
24. Develop, synchronize, and coordinate Theater-wide implementation plans to ensure unity of effort within the entire Theater.
25. Develop integrated program control processes and robust NetOps frameworks for all technology insertions prior to transition to operations and maintenance activities.

26. Transition technology insertion to full operational capability with defined change control processes properly articulated in applicable USCENTCOM regulations in coordination with Operations.
27. Produce decision and information briefings/papers and status frameworks for all applicable projects or processes.
28. Document lessons learned in accordance with CCJ6 policies and procedures.
29. Review and validate component and CJTF C4 network plans and network changes.

C.5.6.1.2 - Multi-National Information Sharing (MNIS) Support

The MNIS development effort was initiated in Fiscal Year (FY) 02 as an immediate special interest program by the OSD to support immediate Combatant Command Coalition Operations following September 11, 2001, and is being continued under this PWS. Examples of Mission Networks in support of MNIS systems include, but are not limited to, USCENTCOM Partner Network, (CPN), Future Mission Network (FMN) and CENTRIXS. These systems enhance the U.S. forces' defense posture and force protection and provide a significant resource for USCENTCOM to use in peace, crisis, war, and operations other than war by allowing collaboration through the sharing of information, e-mail, chat, and common operational picture.

The Contractor shall:

1. Provide on-site program management and coordinates system engineering and technical support necessary to ensure full operational capability of the existing MNIS nodes at USCENTCOM and their associated forward sites. The Contractor shall support operational expansion efforts within USCENTCOM AOR. Provide program management, reviews, development, integration, and coordination of installation necessary to support on-going development of the CENTRIXS Cross Enclave Requirement (CCER), and Mission Networks such as CPN and FMN, and applicable CDS that support MNIS.
2. Analyze the technical impacts of software/hardware maintenance enhancements and/or modifications to the system product baseline and provide technical reports.
3. Develop technical drawings to document the installed implementation of the MNIS system. The drawings shall be entered into the configuration management process established by USCENTCOM and shall include, at a minimum, the interface and systems interface connections, site equipment location drawings, and an updated overall MNIS and network drawings. Drawings shall be delivered in soft copy and also made available via a web-based automated capability.
4. Coordinate site survey, procurement, design, development, communications engineering, installation, implementation, and testing to establish MNIS capabilities within USCENTCOM's AOR. The Contractor shall provide technical reports for each site surveyed with the definitive agreements, plans, and problem areas necessary to ensure a smooth installation into each location. The Contractor shall provide for the configuration documentation for each location.
5. Evaluate COTS/GOTS products that could improve system functionality and/or provide new functionalities in response to user-generated requirements.

C.5.6.2 Chief Information Officer (CIO) Support

The CIO Support Branch (CCJ6-PI) executes the responsibilities of the Office of the USCENTCOM CIO.

The Contractor shall:

1. Advise the CIO regarding a leader-centric, network-enabled enterprise approach to C5 Enterprise and IT application within the Command to ensure USCENTCOM's compliance with applicable legislative, DoD, and Chairman, Joint Chiefs of Staff (CJCS) regulations and directives.
2. Coordinate CIO policy objectives and initiatives with USCENTCOM C5 Enterprise activities.
3. Research, analyze, and review legislative, DoD, OSD, and JS guidance, publications, and policies and provide recommendations to the CIO.
4. Create staff packages and provide documentation including, but not limited to, white papers, information papers, decision papers, point papers, PowerPoint presentations, spreadsheets, databases, webpage design, training and education packages, policy, and guidance IAW USCENTCOM regulations, standards, and processes to facilitate the CIO objectives and intent.
5. Identify gaps in the USCENTCOM C5 Enterprise strategy and associated policies.
6. Create and provide key objectives, policy, governance, and enterprise management of Command Information Resources in accordance with the requirements established by the Clinger-Cohen Act 1996 and other applicable DoD and JS directives.
7. Develop and support the USCENTCOM's C5 Enterprise Strategy, including Command goals for enabling the warfighter and decision makers through the effective application of IT.
8. Develop and support the USCENTCOM's C5 Enterprise Strategy, including Command goals for enabling the warfighter and decision makers through the effective and efficient alignment of IT to the USCENTCOM mission.
9. Develop and support policy and procedures IAW the Information Technology Management Reform Act, 1996, for the management and governance of USCENTCOM Information Resources in order to identify potential gains in effectiveness and efficiencies.
10. Coordinate, track, manage, and sort the Command capability requests, coordinating with the appropriate functional Portfolio Managers (at minimum of eight warfighter and two business mission areas) for validation, prioritization, and alignment of capability requests.
11. Research and propose solutions to enable the modernization of the USCENTCOM IT architecture and integrate new technologies. Monitor emerging technologies and industry best practices and provide recommendation for IT refresh opportunities.

12. Facilitate the tracking of IT expenditures to promote accountability in the USCENTCOM IT Portfolio and to identify and report inconsistencies and/or funding issues.
13. Coordinate, track, and manage compliance with USCENTCOM CIO policy and procedures. When necessary, report non-compliance and recommend actions to address any such non-compliance.
14. Research, review, analyze identified solutions, and draft documents supporting the following USCENTCOM regulations, policies, and strategies: CIO Governance Framework, C5 Enterprise Strategy, IT Life Cycle Management (ITLM), IRM, IT Portfolio Management (IT PfM).
15. Attend working groups, meetings, and conferences to include stateside, overseas, and USCENTCOM's AOR.
16. Coordinate, prepare, and execute the activities of USCENTCOM CIO-directed Working Groups and Boards. This includes preparing the agenda, managing the information in support of the agenda, preparing read-aheads, and publishing minutes from each session.
17. Coordinate, review, analyze, and draft responses to DoD, OSD, JS, USCENTCOM, and Directorate tasks IAW USCENTCOM staffing procedures and guidance.

C.5.6.3 Architectures Support

C.5.6.3.1 Architectures Support

The Contractor shall be the USCENTCOM Enterprise Architecture (EA) developer. This includes researching EA products, developing federated EA products, and providing solutions to USCENTCOM EA issues now and in the future. The USCENTCOM EA shall align to the DoD EA and DoD Joint Capability Area's (JCA) and support process, as well as capability evolution in support of the USCENTCOM IT Portfolio Manager and CIO. This EA developer shall comply with and incorporate existing and future USCENTCOM planning documents, as well as apply Government and industry best standards, to include compliance with the DoD Architecture Framework (DoDAF), modified to appropriately reflect the USCENTCOM environment.

The Contractor shall:

1. Understand Command strategies, missions, roles, functions, and theater support requirements. Performs near-, mid-, and long-term enterprise and strategic C4 planning.
2. Research, develop, and maintain the Command EA including architecture products for operational, system, and technical components.
3. Ensure Contractor team produces warfighter domain architectures that fully address joint/coalition mission threads (operational facilities, tasks, billets, and processes) and current and future Command and Control (C2), Net-Centric, Focused Logistics, Joint Training, Force Application, Force Management, Force Protection, and Battlespace Awareness capabilities.

4. Analyze USCENTCOM architectures, warfighting, business, Enterprise Information Environment (EIE) processes, and IT to identify mission capability gaps, overlaps, and shortfalls; determine and recommend architectural, IT, or process solutions.
5. Research and develop other EA component and architecture documents and plans.
6. Understand and use the DoDAF and other key DoD architecture and net-centric planning instructions.
7. Collect data and coordinate USCENTCOM EA strategic planning throughout the AOR.
8. Review Joint Capabilities Integration Development System (JCIDS) documents, recommendations, and technical input.
9. Identify future technology and Joint Force capabilities and potential architectural and capability impacts for USCENTCOM.
10. Provide recommendations regarding the CCJ6 Strategic Architectures Branch organization and functioning.
11. Understand and use the DoD Architecture Repository System (DARS). Participate in DoD EA conferences, Theater/Component communications conferences, and Command, Control, Communications, Computers, Intelligences, Surveillance, and Reconnaissance (C4ISR) and Architecture Working Groups.
12. Attend DoD, JS, and Combatant Command meetings.
13. Develop and maintain effective working relationships with the USCENTCOM staff and counterparts at the Office of the Assistant Secretary of Defense (Networks and Information Integration (OASD (NII)), JS, Components, JTF's host-nations, coalition, and other agencies.

C.5.6.3.2 - Solution Architecture and Joint Capabilities Integration Development System (JCIDS) Analysis Support

The Contractor shall provide JCIDS analysis of IT Solution Architectures. This includes researching C5 capabilities, IT products, developing IT Solution Architectures and command positions relative to C5 architecture issues now and in the future. IT Solution Architectures and JCIDS analysis through use of Joint C4I Program Assessment Tool – Empowered (JCPAT-E) shall support DoD JCAs and address net-centric evolution in support of the USCENTCOM J6/CIO. This EA JCIDS/Solution Architect shall comply with and incorporate existing and future USCENTCOM planning documents, as well as apply Government and industry best standards, to include compliance with the DoDAF.

The Contractor shall:

1. Develop, recommend, and advance USCENTCOM CCJ6/CIO positions through formal review and evaluation of JCIDS documents.
2. Prepare Command responses to JS or OSD regarding JCIDS documents and associated functional analyses, concept documents, and architectures.
3. Prepare supporting documentation for J6 staff to participate and represent command positions on key issues at strategic DoD conferences, working groups, boards, and

forums to include Senior Warfighters' Forum (SWarF), Functional Capabilities Board (FCB), Integrated Priority List (IPL) conferences, etc.

4. Produce Solution Architectures in support of emergent technology analysis and evaluation of potential solutions to satisfy identified capability gaps and shortfalls, using Joint Command and Control Architecture Capabilities Assessment Environment (JACAE) as a development tool and the DoDAF as a guide.
5. Produce Solution Architectures in support of Joint Urgent Operational Needs Statements (JUONS).
6. Produce Solution Architectures in support of CCJ6/CIO strategic and transition plans, aligning to command functional portfolios and EA.
7. Work with Program / Project / Product Management offices to mitigate operational and technical risk and align strategic business objectives with operational requirements.
8. Perform research and data collection in support of associated Strategic, JCIDS, and Solution Architecture tasks.
9. Work with Command Enterprise architects to ensure alignment and conformance to common standards and semantics.
10. Develop briefings, position papers, and other supporting staff artifacts.

C.5.6.4 Knowledge Management (KM) Support (OPTIONAL CLIN x002)

The USCENTCOM Knowledge Management (KM) office is responsible for USCENTCOM's KM Program this includes developing, maintaining, and integrating KM activities within HQ USCENTCOM and the components and providing training and awareness of KM within USCENTCOM. The USCENTCOM KM Program develops and integrates systems to support day-to-day Government garrison operations, as well as transition quickly to reliable wartime support for the CFH. Web pages, databases, and interfaces reside on JWICS, SIPRNet, NIPRNet, and CENTRIXS networks. The Contractor shall advise and assist the Government operate, monitor, manage, maintain, and develop USCENTCOM's KM Program within the scope of this task.

KM Program and Project Management

The Contractor shall:

1. Advise and assist in developing USCENTCOM's KM Program to include development of Goals, Objectives, Mission, KM Measures, Vision and Implementation/Strategy plans or other associated or related plans.
2. Advise and assist in the preparation and development of KM Project Plans; this may include preparing information papers/reports and presentations on KM projects.
3. Assist in the development of cost metrics for future KM programs and/or projects.
4. Advise and assist in the development, monitoring, and execution of any KM assessment programs or studies.

5. Provide project management expertise on KM initiatives within USCENTCOM; this includes, but is not limited to, monitoring the KM programs and/or projects and providing recommendations to integrate cross-directorate KM projects.
6. Assist in the development/approval of appropriate software design for web content.
7. Analyze applications and obtain feedback from customers to ensure KM applications remain current and are still used.
8. Develop marketing campaign to ensure newly assigned personnel are familiar with locally developed applications.
9. Conduct detailed analysis and identification of operational processes and procedures.
10. Identify and document processes that could be handled by business logic within the Command portal.
11. Engage stakeholder community to ensure successful transition and acceptance of KM processes and procedures.
12. Interface regularly with USCENTCOM and Component personnel.
13. Develop briefings, SDD, and any other artifacts after all meetings in support of the development of KM processes and procedures.
14. Originate/research documentation that outlines the organization's SOPs, business rules, and current KM policies.
15. Document all data/information gathered and develop information flow models.
16. Communicates complex information orally, in writing, and by VTC.
17. Draft, edit, and critique colleague's written communications; comments and coordinates on HQ USCENTCOM directives, policy memorandums, and other staff actions.
18. Routinely attend and actively participate in high-level meetings, conferences, and seminars with Command leadership, JS, and interagency to advocate KM processes and programs in support of HQ USCENTCOM, Component Commands, and deployed JTFs.

KM Exercises and Operations

The Contractor shall:

1. Provide expertise and assistance in the development of Information/Process Models in support of USCENTCOM and its components. Provide analytical expertise in refining organization processes especially as it relates to USCENTCOM Campaign Planning Tasks.
2. Advise and assist by providing operational research expertise with a special focus on the decision making and information flow as it relates to USCENTCOM's KM program.
3. Advise and assist in the development of KM plans to support USCENTCOM's exercise requirements.
4. Provide KM expertise during USCENTCOM exercises or crisis action events.
5. Provide assistance in collecting and organizing USCENTCOM's Lessons Learned Program.
6. Develop process improvement criteria in support of USCENTCOM operational goals in support of exercise and real-world activity.

7. Perform continual assessments and evaluations of HQ USCENTCOM, Component Command, and JTF strategic goals and objectives in an effort to optimize KM capabilities in support of the Combatant Commander's decision making processes.
8. Establish relationships with other Combatant Command KM teams to identify best practices in an effort to improve KM standards at HQ USCENTCOM and across the Federal Government.

KM Policy and Training Program

The Contractor shall:

1. Advise and assist in the development and monitoring of the USCENTCOM's KM Training and Awareness Program. This shall include developing a KM training program and providing the training if requested by the Government.
2. Advise and assist on the development of policies and training programs associated with portal content management; provide recommendations on how to improve content management.
3. Advise and assist in the development of KM related policies and procedures. Assist in the development of USCENTCOM's response to DoD policy initiatives.
4. Develop and maintain KM Concepts of Operations and regulations.
5. Develop, maintain, and facilitate the implementation of KM policies and procedures; identify program and process requirements; and ensure alignment of KM activities to USCENTCOM mission, goals, and objectives.

KM Technology and Initiation Program

The Contractor shall:

1. Develop plans and recommendations on how to better utilize existing KM systems, technology suites or collaboration tools.
2. Provide best practice recommendations on the management and design of portal systems to enhance the USCENTCOM KM Program.
3. Provide recommendations and assistance in the development of innovation and technology plans that supports the USCENTCOM mission and KM goals.
4. Provide key inputs to command strategy and policy development to successfully transform HQ USCENTCOM into a learning organization that is flexible, agile, and receptive to change.
5. Remain abreast of new technologies and processes in the data analysis, production, and dissemination arena in order to constantly improve, plan, and coordinate their migration into the USCENTCOM KM architecture.
6. Provide guidance for the design and conduct of comprehensive studies, to determine effectiveness of operations, flow of information, and effectiveness of KM systems across all levels of the Command.

7. Conduct research in the areas of KM, process improvement, technology, and/or organizational learning to increase the knowledge base of HQ USCENTCOM; provide improved tools and methodologies to enable the HQ USCENTCOM staff, Component Commands, JTFs, and external partners and agencies in a collaborative environment.
8. Develop critical information processing tools and techniques to enhance and empower the implementation of HQ USCENTCOM KM initiatives.
9. Prepare written materials on request such as USCENTCOM Commander, Deputy Commander, and Chief of Staff Memorandums and directives, as well as other brochures, CDs, and web-based content that direct and optimize KM processes within the Command.
10. Provide predictive KM strategy based upon research of benchmarks from both the private and public sector to ensure that HQ USCENTCOM stays on the leading edge in the KM field.

C.5.7 TASK AREA 7 – RESOURCE MANAGEMENT SUPPORT

C.5.7.1 Records Management

Operations Iraqi Freedom (OIF), New Dawn (OND) and Enduring Freedom (OEF) have resulted in the mass migration of millions of documents back to USCENTCOM, which takes over the responsibility of managing this record material at the end of a mission. Concomitantly, USCENTCOM will take over the responsibility of managing record material from future contingency events.

The Contractor shall provide electronic records analysis and support to the Command in organizing and managing this massive digital collection for preservation purposes in order to meet legal obligations under the Federal Records Act. Additionally, the Contractor is responsible for assisting in the implementation of Total Records and Information Management (TRIM) and updated versions to the Directorates/Special Security Office (SSO) both at HQ USCENTCOM and CFH. The Contractor shall be responsible for working on setting up document queues based on each Directorates file plan so records can be mapped into TRIM as part of an automatic process. The Contractor shall support the TRIM/SharePoint integration as part of a greater KM Program initiated by the Chief of Staff.

The Contractor shall provide records management support of the OIF and OND War Records migration, including work on organizing records the Command receives from OIF/OND, purging redundant records, migrating final records into TRIM, and adding required metadata to documents so records are properly tagged for quicker research and retrieval.

Specifically, the Contractor shall;

1. Work with CCJ6-R and CCJ6-E (USCENTCOM Engineering Division) staff on the integration of TRIM and MS SharePoint 2010.
2. Work with the CCJ6-RDR (Records Management Section) Section Chief in the development of information taxonomy for all U.S. Forces-Iraq (USF-I) Records and

make recommendations to the existing records taxonomical structure currently used within TRIM.

3. Train all CCJ6-R personnel and any other USCENTCOM records staff on TRIM 7.1. Training should elevate the trainee to the TRIM Administrator level.
4. Work with CCJ6-R and SJS staff in the management of Tasker Tool records into TRIM.
5. Work with TRIM and Task Management Tool (TMT) vendors to work on integration between the two products.
6. Assist in the development of an email records solution for all USCENTCOM GO/FO email by capturing emails from the back end without the GO/FO having the knowledge to use TRIM to store his/her records.
7. Assist CCJ6-R personnel in working with Active Navigation to better improve the document analysis of the OIF/OND collections.
8. Assist in the troubleshooting of any TRIM-related issues, including the expansion of TRIM usability to CENTCOMs SCO offices.
9. Assist CCJ6-RDR in the transfer of records to the National Archives via the TRIM Export utility and work on a PDF batch conversion methodology for the Command.

C.5.7.2 Asset Management

C.5.7.2.1 Asset Management of USCENTCOM HQ

USCENTCOM requires Inventory Control Analysis support to maintain consistent accountability of ADPE assets supporting HQ USCENTCOM. The Contractor shall assist with the operation of the Project Support Facility at the HQ's per written procedures provided by the Government and perform shipping and receiving of ADPE assets, storage of computer/communications-related assets, and distribution of hardware in conjunction with Government-delivered distribution plans at HQ, in support of the AOR. The Contractor shall ensure that all IS ADPE hardware and software are properly received, documented, stored, and disbursed to the required user to maintain good supply and accountability of ADPE. The Contractor is responsible for asset inventories at the Project Support Facility normal coverage for this task are 5 days a week from 0800-1700.

The Contractor shall:

1. Responsible for receiving, labeling and properly documenting all incoming equipment.
2. Responsible for the distribution and shipping of all ADPE equipment at the HQ and the AOR.
3. Ensure all property items are uniquely labeled, tracked and changes inputted into the database.
4. Inspect goods and materials and assess condition for distribution/recycling.
5. Coordinate the disposal of property, supplies, and or material in compliance with Government and/or military regulations/guidelines.
6. Maintain records of acquisition/distribution and property, supplies, and materials.
7. Investigate and reconcile discrepancies.

8. Process excess APDE as identified by CCJ6 using DoD procedures.
9. Maintain accountability and separation of CCJ6 Directorate project Bill-of-Materials.

C.5.7.2.2 Asset Management at USCENTCOM CFH

USCENTCOM requires Inventory Control Analysis support to maintain consistent accountability of ADPE assets supporting HQ USCENTCOM. The Contractor shall operate the Asset Management Facility at CFH per written procedures provided by the Government to perform shipping and receiving of ADPE assets, storage of computer/communications-related assets, and distribution of hardware in conjunction with Government-delivered distribution plans at CFH, in support of Bahrain, Qatar, and Kuwait. The Contractor shall ensure that all IS ADPE hardware and software are properly received, documented, stored, and disbursed to the required user to maintain good supply and accountability of ADPE. The Contractor is responsible for asset inventories at CFH, Bahrain, and Kuwait. Normal coverage for this task are 7 days a week from 0700-1900.

The Contractor shall:

1. Schedule and revise shipment plans to ensure efficient distribution of products to satisfy customers. Analyze inventory levels, production speed, and product demand to determine reorder levels, which shall ensure product availability and minimize inventory costs.
2. Manage inventory levels to efficiently utilize capital investment while maintaining adequate coverage for known/projected demand.
3. Maintain control and accountability over assigned products; determine appropriate distribution based on lead times and demand.
4. Handle the acquisition of property, supplies, and/or materials from other agencies, to include transporting and storage.
5. Ensure all property items are uniquely identified and changes are tracked and recorded.
6. Inspect goods and materials and assess condition for distribution/recycling.
7. Coordinate the disposal of property, supplies, and or material in compliance with Government and/or military regulations/guidelines.
8. Maintain records of acquisition/distribution and property, supplies, and materials.
9. Investigate and reconcile discrepancies.
10. Process computer assets to/from the SSOs in the AOR when equipment is going from CFH.
11. Process excess APDE as identified by CCJ6 using DoD procedures.
12. Maintain accountability and separation of CCJ6 Directorate project Bill-of-Materials.
13. Aid each Directorate with completing quarterly and annual inventories.
14. Help research and reconcile any inventory discrepancies.

TASK AREA 8 – EXTENDED WORK WEEK (EWW) / SURGE SUPPORT

Extended Work Week / Surge support shall be in addition to the TO core sustainment requirements, but inclusive of implementation of approved technology initiatives (i.e., technical insertions). The Contractor shall be prepared to provide support for short-term as-neeeded support requirements including system, system component, or application failure; systems integration; systems deployment; and training. Examples of EWW / surge requirements include, but are not limited to, augmenting high-level CND initiatives to battle cyber-attacks on the USCENTCOM and related networks, USCENTCOM Commander and the C4 Systems Director initiatives and exercises to improve and streamline the IT enterprise, and augmentation of the existing force in addressing communications and IT projects in the USCENTCOM AOR. The surge occurrences will be of a limited duration based on individual circumstances.

This surge support may require the use of outside, corporate 'reach-back' support to fix urgent issues in the course of a day to projects lasting several months. The contractor shall provide emergency technical support worldwide on short notice (e.g., two (2) workdays). It is anticipated that a typical team may include contractor personnel for a specified period of time to provide support for urgent requirements.

The contractor shall also be available 24 hours a day, 7 days a week "on-call" support. The contractor shall adhere to a robust industry standard for "on-call" support to include appropriate response times for solving problems based on mission criticality and priority as determined by the Government.

Unscheduled support requirements must be processed on an expedited basis.

The Contractor shall not provide technical support outside the scope of this TO and shall only use the labor categories within the Alliant base contract. The use of higher skilled personnel to perform these duties shall be approved by the Government before incurrence. Deliverables for these efforts may include technical presentations, reports, and other technical products.

SECTION D - PACKAGING AND MARKING

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract. Only those Sections listed from the Alliant Basic apply to this Task Order.

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract. Only those Sections listed from the Alliant Basic apply to this Task Order. In addition, the following applies:

E.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

The following clauses apply to this Task Order. This Task Order incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

https://www.acquisition.gov/far/index.html

CLAUSE #	CLAUSE TITLE	DATE
52.246-5	INSPECTION OF SERVICES—COST REIMBURSEMENT	APR 1984
52.246-16	RESPONSIBILITY FOR SUPPLIES	APR 1984

E.2 PLACE OF INSPECTION AND ACCEPTANCE

Inspection of all work performance, reports, and other deliverables under this TO shall be performed by the USCENTCOM TPOC.

Acceptance of all work performance, reports, and other deliverables under this TO shall be performed by the FEDSIM Contracting Officer's Representative (COR).

E.3 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to TO requirements by the FEDSIM COR. Inspection may include validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the TO. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

E.4 BASIS OF ACCEPTANCE

The basis for acceptance shall be in compliance with the requirements set forth in the TO, the Contractor's proposal and other terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

For software development, the final acceptance of the software program will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected.

If the draft deliverable is adequate, the Government may accept the draft and provide comments for incorporation into the final version.

All of the Government's comments on deliverables must either be incorporated in the succeeding version of the deliverable, or the Contractor must demonstrate to the Government's satisfaction why such comments should not be incorporated.

If the Government finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the requirements stated within this TO, the document may be immediately rejected without further review and returned to the Contractor for correction and resubmission. If the Contractor requires additional Government guidance to produce an acceptable draft, the Contractor shall arrange a meeting with the FEDSIM COR.

E.5 DRAFT DELIVERABLES

The Government will provide written acceptance, comments, and/or change requests, if any, within 15 workdays (unless specified otherwise in Section F) from Government receipt of the draft deliverable. Upon receipt of the Government’s comments, the Contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

E.6 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The CO/COR will provide written notification of acceptance or rejection (Section J, Attachment O) of all final deliverables within 15 workdays (unless specified otherwise in Section F). All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

E.7 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the Contractor, within ten workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the Contractor will immediately notify the FEDSIM COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

If the Contractor does not provide products or services that conform to the requirements of this TO, the Government will document the issues associated with the non-conforming products or services in the award fee determination report, and there will be an associated reduction in the earned award fee.

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract. Only those Sections listed from the Alliant Basic apply to this Task Order. In addition, the following applies:

F.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

The following clauses apply to this Task Order. This Task Order incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this address:

https://www.acquisition.gov/far/index.html

CLAUSE #	CLAUSE TITLE	DATE
52.242-15	STOP-WORK ORDER	AUG 1989
52.242-15	ALTERNATE I	APR 1984

F.3 TASK ORDER PERIOD OF PERFORMANCE

The period of performance for this TO is a one-year base period and four, one-year options.

Base Period	September 7, 2012 thru September 6, 2013
Option Yr 1	September 7, 2013 thru September 6, 2014
Option Yr 2	September 7, 2014 thru September 6, 2015
Option Yr 3	September 7, 2015 thru September 6, 2016
Option Yr 4	September 7, 2016 thru September 6, 2017

F.4 PLACE OF PERFORMANCE

The primary place of performance for this TO shall be the HQ USCENTCOM facility at MacDill AFB in Tampa, Florida and other U.S. Government facilities or operational locations in the USCENTCOM AOR or other supported COCOM AORs. The Government may require Contractor personnel to travel to remote locations throughout USCENTCOM AOR.

All labor in CONUS and Bahrain is based on a 40 hour work week. All labor in Qatar is based on a 60 hour work week. However, Contractor personnel shall work Extended Work Week hours when necessary to accomplish compelling requirements.

The required duty hours for each task are as depicted in the following table:

Task	Description	On-Site Support
5.2	C4 Systems Support	
5.2.1	C3 Systems Support	

5.2.1.1	Management of HQ Systems Infrastructure	24x7x365
5.2.1.2	Voice Services	M-F 0700-1700*
5.2.1.3	Patch and Test Facility (PTF) Support	24x7x365
5.2.1.4	Cable Plant Support	M-F 0700-1800*
5.2.2	Enterprise Network Services Support	
5.2.2.1	Communications Support	24x7x365
5.2.2.2	GCCS Support	24x7x365
5.2.2.3	End-User Information Technology Support	24x7x365
5.2.2.4	Server Maintenance Support	24x7x365
5.2.2.5	Wireless Support	M-F 0600-1800*▲
5.2.3	Operations Support	
5.2.3.1	Visual Information Systems	M-F 0600-1700*▽
5.2.3.2	Security Cooperation Offices (SCO) Support	M-F 0500-1700*▲
5.2.4	Customer Support Operations	24x7x365
5.2.5	Commander Communications Support	M-F 0800-1800*
5.2.6	HQ User Training	M-F 0800-1700*
5.3	Theater Network Operations (NetOps) Support	
5.3.1	Level 0 Fault Monitoring, Identification, Resolution	24x7x365
5.3.2	Level 1 Current Operations	24x7x365
5.3.3	Information Assurance – CND	24x7x365
5.4	Engineering Support	
5.4.1	Project Management	M-F 0700-1800
5.4.2	Engineering Support	
5.4.2.1	Engineering and Technology Support	M-F 0700-1800
5.4.2.2	Engineering Design Analysis	M-F 0700-1800
5.4.2.3	Coalition Network Architecture Engineering	M-F 0700-1800
5.2.3.4	Configuration and Enterprise License Management	M-F 0700-1800
5.4.2.5	Engineering Monitoring Tools Support	M-F 0700-1800
5.4.2.6	Change Management	M-F 0700-1800
5.4.3	Engineering, Test, Analysis and Integration Lab	M-F 0700-1800
5.4.4	Software Engineering Support	M-F 0700-1800
5.5	Cyber Support	
5.5.1	Headquarters Network Defense	24x7x365
5.5.2	Theater Cyber Initiatives	M-F 0700-1800*
5.5.3	Cyber Certification and Accreditation	M-F 0700-1800*
5.6	Programs and Architectures Support	
5.6.1	Programs and Architectures	
5.6.1.1	Program Planning and Development Support	M-F 0800-1700
5.6.1.2	Multi-National Information Sharing (MNIS) Support	M-F 0800-1700
5.6.2	Chief Information Officer (CIO) Support	M-F 0800-1700
5.6.3	Architectures Support	
5.6.3.1	Architectures Support	M-F 0800-1700
5.6.3.2	Solution Architecture and JCIDS Analysis Support	M-F 0800-1700
5.6.4	Knowledge Management (OPTIONAL TASK)	M-F 0800-1700
5.7	Resource Management Support	
5.7.1	Records Management Support	M-F 0800-1700
5.7.2	Asset Management Support	M-F 0800-1700

*On-call support shall be provided outside of duty hours, with a maximum time for reporting to duty station after on-call support is requested of one hour from time of notification. A comprehensive on-call/alert roster shall be maintained and updated on a monthly basis.
▽Mission critical and mission essential VIS events outside of normal duty hours shall be adequately staffed in HQ and CFH, where applicable.
▲ Contractor shall also have 24x7x365 remote support capabilities.

The contractor shall provide the following coverage in CFH under normal operating conditions. On call support for these tasks shall be provided outside of duty hours tto support emergency conditions, outages and events. All time refers to local time.

Task	Description	CFH Support
5.2.1	C3 Systems Support	
5.2.1.1	Management of HQ Systems Infrastructure	M-Sa 0900-1900
5.2.1.2	Voice Services	M-Sa 0900-1900
5.2.1.3	Patch and Test Facility (PTF) Support	M-Sa 0900-1900
5.2.2	Enterprise Network Services Support	
5.2.2.3	End-User Information Technology Support	M-Sa 0900-1900
5.2.2.4	Server Maintenance Support	M-Sa 0700-1900
5.2.3	Operations Support	
5.2.3.1	Visual Information Systems	M-Sa 0700-1900
5.2.4	Customer Support Operations	M-Sa 0700-1900
5.5	Cyber Support	
5.5.1	Headquarters Network Defense	M-Sa 0900-1900
5.7	Resource Management Support	
5.7.2	Asset Management Support	M-F 0800-1700

F.5 DELIVERABLES

The following schedule of milestones will be used by the FEDSIM COR to monitor timely progress under this TO. The following abbreviations are used in this schedule:

NLT: No Later Than
TOA: Task Order Award
All references to Days: Government Workdays

Deliverables are due the next Government workday if the due date falls on a holiday or weekend.

The Contractor shall submit the deliverables listed in the following table:

TASK AREA 1 – PMO SUPOPORT

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Project Start (PS)	X001	C.5.1.1	At TOA
Integrated Master Schedule	X001	C.5.1.1	IAW PMP
Task Order Kick-Off Meeting	X001	C.5.1.1	10 workdays after TOA
Final Transition – In Plan	X001	C.5.1.9	10 workdays after TOA
Final Quality Control (QCP) Plan	X001	C.5.1.7	10 workdays after TOA
Program Management Plan (PMP)	X001	C.5.1.4	
Draft PMP	X001	C.5.1.4	10 workdays after TOA
Final PMP	X001	C.5.1.4	10 workdays after Government comment
Disaster Recovery Plan	X001	C.5.1.5	30 workdays after TOA
Financial Status Report	X001	C.5.1.1.3	Monthly
Monthly Status Report (MSR)	X001	C.5.1.2	10th workday of each month
Transition – Out Plan	X001	C.5.1.10	90 calendar days prior to the expiration of Task Order

TASK AREA 2 - C4 SYSTEMS SUPPORT

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Inventory of all assets and spare equipment	X001	C.5.2	Monthly
Master Station Log (MSL) and shift change procedures	X001	C.5.2	Daily
PMI completion documents.	X001	C.5.2	IAW PMP
Preventive maintenance schedule.	X001	C.5.2	Monthly
Security accreditation documentation for all systems/networks	X001	C.5.2	IAW PMP
Documentation and artifacts required to support inspections for any network/system	X001	C.5.2	IAW PMP
Prioritized Service Restoration List.	X001	C.5.2	Quarterly
Physical and logical diagrams	X001	C.5.2	Monthly
Continuity Folder	X001	C.5.2	IAW PMP
Operational Checklists documenting standard tactics, techniques and procedures (TTPs) for executing tasks	X001	C.5.2	30 days after award and updated IAW PMP
Consolidated folder of lessons learned during troubleshooting, best practices, TTPs, policies and procedures	X001	C.5.2	IAW PMP
After Action Report	X001	C.5.2	COB next business day
Documentation including site surveys, COAs, drawings, cost and time estimates and assembled material lists	X001	C.5.2	IAW PMP

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Verification/update Report of the Telephone Subscriber Database	X001	C.5.2.1.2	Bi-annually
Telephone Directories Update	X001	C.5.2.1.2	Quarterly
Telecommunications and Monitoring Assessment Program (TMAP) inspection report	X001	C.5.2.1.2	Annually
Consolidated collection of documents for relevant systems and technologies	X001	C.5.2.1.3	Quarterly
Physical cabling diagrams for all USCENTCOM	X001	C.5.2.1.4	Monthly
Chain of Custody Logs for SPECAT messages.	X001	C.5.2.2.1	IAW PMP
DMS software and hardware configuration control and licensing repository	X001	C.5.2.2.1	60 days after award and updated monthly
Server Security Report (including IAVA compliance status information).	X001	C.5.2.2.4	IAW PMP
Server Health Report	X001	C.5.2.2.4	Monthly or IAW PMP
Server Status Report	X001	C.5.2.2.4	Monthly or IAW PMP
Primary and alternate Personal Wireless Communications Manager (PWCS) documentation	X001	C.5.2.2.5	IAW PMP
Cell Phone Billing Analysis and Cost Reduction recommendations	X001	C.5.2.2.5	IAW PMP
Project, trip, and phase completion reports	X001	C.5.2.3.2	IAW PMP
Update SCO website	X001	C.5.2.3.2	Monthly
Log of technical assistance requests and their status	X001	C.5.2.3.2	Monthly
Incident status report	X001	C.5.2.4	Daily
Customer survey analysis report.	X001	C.5.2.4	Weekly
Knowledge base for investigating, diagnosing and resolving Tier 1 incidents	X001	C.5.2.4	Monthly
CSO Concept of Operations (CONOPS).	X001	C.5.2.4	Bi-annually
Trend analysis of common incidents, trouble ticket/Customer Request (CR)/Work Order (WO) status updates, incident key performance indicators.	X001	C.5.2.4	IAW PMP
Inventory of all equipment included in deployable communications suites and any spare equipment	X001	C.5.2.5	Monthly

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Course curriculum and training materials	X001	C.5.2.6	IAW PMP
Training schedules	X001	C.5.2.6	Monthly
Metrics and trend analyses of course and instructor	X001	C.5.2.6	Monthly

TASK AREA 3 – Theater Network Operations (Net) Support

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Activity reports	X001	C.5.3	Weekly
Network situational update briefs	X001	C.5.3	Daily
Network situational deep dive analysis to government leadership	X001	C.5.3	IAW PMP, weekly depending on network condition
Iterative continual service improvement meetings	X001	C.5.3	Weekly
Generate trouble tickets on all activity in order to facilitate trend analysis and maintain historical record of events	X001	C.5.3	IAW PMP, several per day
Incident/Event/ Problem Quad Chart	X001	C.5.3	IAW PMP, several per week

TASK AREA 4 – Engineering Support

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Software Design Documents (SDD)	X001	C.5.4.4	IAW PMP
SQL Databases	X001	C.5.4.4	IAW PMP
Reports (Using SQL Reporting Tool)	X001	C.5.4.4	IAW PMP
Command Level Web Pages	X001	C.5.4.4	IAW PMP
Requirements Packages	X001	C.5.4	IAW PMP
Security Assessment	X001	C.5.4.2 & C.5.4.3	IAW PMP
Change Requests	X001	C.5.4	IAW PMP
Business Cases	X001	C.5.4.2, C.5.4.3 & C.5.4.4	IAW PMP
Equipment and User Trends Analysis Reports	X001	C.5.4.2.5	IAW PMP
Configuration Management Policy Document Updates	X001	C.5.4.2.4	IAW PMP
Change Management Policy Document Updates	X001	C.5.4.2.4	IAW PMP
Command Approved Hardware/Software List	X001	C.5.4.2.4	Maintained Continuous
Engineering and Design Documentation	X001	C.5.4.2, C.5.4.3	IAW PMP

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
		& C.5.4.4	
Network Performance Reports	X001	C.5.4.2.5	Daily / Weekly / Monthly / Quarterly
Proof-of-Concept Demonstrations	X001	C.5.4.2	
System Administrator and User Guidance	X001	C.5.4.2 & C.5.4.3	IAW PMP
Architectural Diagrams	X001	C.5.4.2, C.5.4.3 & C.5.4.4	IAW PMP
Central Diagrams Repository	X001	C.5.4.2.5	Maintained Continuous
Information Paper	X001	C.5.4	IAW PMP
Stakeholder's Contact List	X001	C.5.4.1	IAW PMP
Engineering Implementation Plan	X001	C.5.4.2 & C.5.4.3	IAW PMP
Engineering Test Plan	X001	C.5.4.2	IAW PMP
Concept of Operations	X001	C.5.4	IAW PMP
Lessons Learned	X001	C.5.4	IAW PMP
Plan of Actions & Milestones (POAM)	X001	C.5.4	IAW PMP
Site Surveys	X001	C.5.4	IAW PMP
Predictive Analysis (CCR 25-200 Review)	X001	C.5.4	IAW PMP
Executive Level Status Presentations	X001	C.5.4	IAW PMP
Weekly Activity Reports (WAR)	X001	C.5.4	Weekly
Ticketing Response Reports	X001	C.5.4	Monthly

TASK AREA 5 – Cyber Support

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Operational Checklists documenting standard tactics, techniques and procedures (TTPs) for executing tasks required to support cyber security operations	X001	C.5.5	30 days after award and as required
Best Practices, Policies and Procedures	X001	C.5.5	Quarterly
Continuity Folder	X001	C.5.5	IAW PMP
Trend analysis of security events	X001	C.5.5.1	Monthly
IAVA Compliance Report	X001	C.5.5.1	Within 72 hours of a completed scan
Vulnerability Assessments for new hardware and	X001	C.5.5.3	IAW PMP
Detailed Threat/Capability Reports (based on specified topics)	X001	C.5.5.2	IAW PMP
Network Damage Assessments	X001	C.5.5.2	Within 24 hours after any significant event

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Attack Assessment Report	X001	C.5.5.2	Weekly
Network Security Surveillance Capabilities and Gaps report	X001	C.5.5.2	Quarterly
Theater Cyber Training Program Report	X001	C.5.5.2	Semi-Annually
Cyber Security Trend Analysis report	X001	C.5.5.2	Monthly
CDS Techniques, Technologies and Vulnerabilities Report	X001	C.5.5	IAW PMP
CDS Technical Report	X001	C.5.5	IAW PMP
CDS Systems Report	X001	C.5.5	Monthly
Risk Assessment/Analysis Reports	X001	C.5.5	IAW PMP

TASK AREA 6 – Programs and Architectures Support

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Develop Government Policy	X001	C.5.6.1.1	IAW PMP
Technical Systems Documentation	X001	C.5.6.1.1	IAW PMP
Program Documentation	X001	C.5.6.1.1	IAW PMP
Program Transition Plan	X001	C.5.6.1.1	IAW PMP
USCENTCOM Theater Policy and Guidance	X001	C.5.6.1.1	IAW PMP
POM Data	X001	C.5.6.1.1	IAW PMP
Project Management Charters (PMC)	X001	C.5.6.1.1	IAW PMP
Kick-Off Briefings	X001	C.5.6.1.1	IAW PMP
Project Scope Statements	X001	C.5.6.1.1	IAW PMP
Decision and Information Briefings/Papers	X001	C.5.6.1.1	IAW PMP
Project Management Plans	X001	C.5.6.1.1	IAW PMP
Systems Analysis and Design	X001	C.5.6.1.1	IAW PMP
Certification and Accreditation Documentation	X001	C.5.6.1.1	IAW PMP
Theater-wide Implementation Plans	X001	C.5.6.1.1	IAW PMP
Information Briefings/Papers	X001	C.5.6.1.1	IAW PMP
500 Day Plan	X001	C.5.6.1.1	Annual
History Report	X001	C.5.6.1.1	IAW PMP
Technical Engineering Drawings	X001	C.5.6.1.2	IAW PMP
Site Survey Technical	X001	C.5.6.1.2	IAW PMP
Configuration Documentation	X001	C.5.6.1.2	IAW PMP
Staff Packages	X001	C.5.6.2	IAW PMP
White Papers	X001	C.5.6.2	IAW PMP

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Information Papers	X001	C.5.6.2	IAW PMP
Point Papers	X001	C.5.6.2	IAW PMP
Powerpoint Presentations	X001	C.5.6.2	IAW PMP
Spreadsheets	X001	C.5.6.2	IAW PMP
Databases	X001	C.5.6.2	IAW PMP
USCENTCOM CIO Executive Board (CEB) Agenda, Read-Aheads, and Minutes	X001	C.5.6.2	IAW PMP
Command C5ISR Enterprise Architecture	X001	C.5.6.3.1	Annual
Command Position Supporting Documentation	X001	C.5.6.3.2	IAW PMP
Solution Architectures	X001	C.5.6.3.2	IAW PMP
Administrative Training Material	X001	C.5.6.4	IAW PMP
Technical System Documentation	X001	C.5.6.4	IAW PMP
Program Transition Plan	X001	C.5.6.4	IAW PMP
Policy Development	X001	C.5.6.4	IAW PMP
Kick-off Briefings	X001	C.5.6.4	IAW PMP
Decision and Information Brief Papers	X001	C.5.6.4	IAW PMP
Process Improvement	X001	C.5.6.4	IAW PMP
System Analysis and Design	X001	C.5.6.4	IAW PMP
Staff Packages	X001	C.5.6.4	IAW PMP
White Papers	X001	C.5.6.4	IAW PMP
Point Papers	X001	C.5.6.4	IAW PMP
Power Point Presentation	X001	C.5.6.4	IAW PMP
Spreadsheets	X001	C.5.6.4	IAW PMP
Databases	X001	C.5.6.4	IAW PMP
Lesson learned Analysis	X001	C.5.6.4	IAW PMP
USCENTCOM KIMB/KIMWG/JKIMWG	X001	C.5.6.4	IAW PMP
IAW PMP Standard Operating Procedure (SOP) documents.	X001	C.5.6.4	IAW PMP

TASK AREA 7 – Resource Management Support

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
Status report to include number of records migrated to TRIM	X001	C.5.7.1	Monthly
Status report to include number of USCENTCOM staff trained on TRIM	X001	C.5.7.1	Monthly

MILESTONE/DELIVERABLE	CLIN	PWS REFERENCE	PLANNED COMPLETION DATE
7.1			
Inventory Report	X001	C.5.7.2	Quarterly and Annual

F.5.1 PUBLIC-RELEASE OF CONTRACT DOCUMENTS REQUIREMENT

The Contractor agrees to submit, within ten workdays from the date of the Contracting Officer's execution of the initial TO, or any modification to the TO (exclusive of Saturdays, Sundays, and Federal holidays), a portable document format (PDF) file of the fully executed document with all proposed necessary redactions, including redactions of any trade secrets or any commercial or financial information that it believes to be privileged or confidential business information, for the purpose of public disclosure at the sole discretion of GSA. The Contractor agrees to provide a detailed written statement specifying the basis for each of its proposed redactions, including the applicable exemption under the Freedom of Information Act (FOIA), 5 U.S.C. § 552, and, in the case of FOIA Exemption 4, 5 U.S.C. § 552(b)(4), shall demonstrate why the information is considered to be a trade secret or commercial or financial information that is privileged or confidential. Information provided by the Contractor in response to the contract requirement may itself be subject to disclosure under the FOIA. Submission of the proposed redactions constitutes concurrence of release under FOIA.

GSA will carefully consider all of the Contractor's proposed redactions and associated grounds for nondisclosure prior to making a final determination as to what information in such executed documents may be properly withheld.

F.5.2 DELIVERABLES MEDIA

The Contractor shall deliver all electronic versions by email and CD-ROM, as well as placing in the USCENTCOM's designated repository. The following are the required electronic formats, whose versions must be compatible with the latest, commonly available version on the market.

- Text MS Word
- Spreadsheets MS Excel
- Briefings MS PowerPoint
- Drawings MS Visio
- Schedules MS Project

F.5.3 SPECIAL DELIVERABLES FORMAT

All documentation produced and delivered in support of the USCENTCOM mission for this task order shall be formatted in accordance with USCENTCOM Regulation (CCR) 25-30, "Information Management – Preparation of Administrative Publications" and follow USCENTCOM Action Officer (AO) templates of standards. These standards are maintained at the USCENTCOM Secretary of the Joint Staff (SJS) Portal resident on the classified USCENTCOM network. Exceptions are task order status and plan deliverables normally delivered directly to the GSA CO, GSA COR and Technical Point of Contact (TPOC)."

F.6 PLACE(S) OF DELIVERY

Unclassified deliverables and correspondence shall be electronically delivered to the GSA Contracting Officer (CO), Contracting Officer's Representative (COR) and Technical Point of Contact (TPOC) at the following addresses:

Denise VonDibert
Contracting Officer (CO)
Email: denise.vondibert@gsa.gov

Timothy R. Bowers, PMP
Contracting Officer's Representative (COR)
Email: timothy.bowers@gsa.gov
timothy.bowers@centcom.mil

Joseph Taylor
Technical Point of Contact (TPOC)
joseph.taylor@centcom.mil

Classified deliverables shall be electronically delivered to the GSA Contracting Officer's Representative (COR) at the following address:

Timothy R. Bowers, PMP
Contracting Officer's Representative (COR)
Email: timothy.bowers@centcom.smil.mil

F.7 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT (PNR)

The Contractor shall notify the FEDSIM COR via a Problem Notification Report (PNR) (Section J, Attachment K) as soon as it becomes apparent to the Contractor that a scheduled delivery will be late. The Contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The FEDSIM COR will review the new schedule and provide guidance to the Contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract. Only those Sections listed from the Alliant Basic apply to this Task Order. In addition, the following applies:

G.3 ROLES AND RESPONSIBILITIES

This section describes the roles and responsibilities of Government personnel after Task Order Award:

G.3.5 CONTRACTING OFFICER'S REPRESENTATIVE

The CO will appoint a COR in writing for each TO. The COR will receive, for the Government, all work called for by the TO and will represent the CO in the technical phases of the work. The COR will provide no supervisory or instructional assistance to Contractor personnel.

The COR is not authorized to change any of the terms and conditions, scope, schedule, and price of the Contract or the TO. Changes in the scope of work will be made only by the CO by properly executed modifications to the Contract or the TO.

G.3.5.1 CONTRACT ADMINISTRATION

Contracting Officer (CO)

Denise VonDibert
1800 F St NW
Washington, DC 20405
Tel: 703- 589-2643
Fax: 703 605-9987
Email: Denise.VonDibert@gsa.gov

Contracting Officer's Representative (COR)

Timothy R. Bowers, PMP
IT Management Specialist
GSA / FAS / AAS / FEDSIM
7115 South Boundary Blvd, CTF 210
MacDill AFB, FL 33621-5101
Desk: 813-529-6677
Fax: 813-827-6332
Email: timothy.bowers@gsa.gov
timothy.bowers@centcom.mil

Technical Point of Contact (TPOC):

Joseph Taylor
USCENTCOM / CCJ6-RA
7115 South Boundary Blvd, CTF 210
MacDill AFB 33621-5101

G.4 EXTENDED WORK WEEK PROVISIONS

If continued support (beyond a standard 40-hour work week) is necessary to support the requirements, Contractor employees may be required to work an Extended Work Week (hours in excess of 40 per week). The Extended Work Week requires both FEDSIM COR and the Contractor management approvals and is utilized where exempt staff are required to work extended hours due to such as accelerated project schedule or exigent circumstances, or to work in conditions under which the employee cannot dictate his/her personal work schedule. The contractor shall provide to the FEDSIM PM an explanation as to why the work cannot be performed during normal duty hours, and the effect if not approved. For Extended Work Week, exempt staff are paid, and the contractor shall be entitled to reimbursement for, a pro rata share (straight time) of their weekly salary based on the extended hours worked. The labor rates charged will not be in excess of the current negotiated rates.

G.9.6 INVOICE SUBMISSION

The Contractor shall submit Requests for Payments in accordance with the format contained in General Services Administration Acquisition Manual (GSAM) 552.232-25, PROMPT PAYMENT (NOV 2009), to be considered proper for payment. In addition, the following data elements shall be included on each invoice.

Task Order Number: *(from GSA Form 300, Block 2)*
Paying Number: *(ACT/DAC NO.) (From GSA Form 300, Block 4)*
FEDSIM Project Number: 11041DEM
Project Title: USCENTCOM C4 Enterprise Support

The Contractor shall certify with a signed and dated statement that the invoice is correct and proper for payment.

The Contractor shall provide invoice backup data in accordance with the contract type, including detail such as labor categories, rates, and quantities of labor hours per labor category.

The Contractor shall submit invoices as follows:

The Contractor shall utilize FEDSIM's electronic Tracking and Ordering System (TOS) to submit invoices. The Contractor shall submit invoices electronically by logging onto the following link (requires Internet Explorer to access the link):

https://portal.fas.gsa.gov

Select *Vendor Support*, log in using your assigned ID and password, then click on *Create Invoice*. The TOS Help Desk should be contacted for support at 877-472-4877 (toll free). By utilizing this method, no paper copy of the invoice shall be submitted to GSA FEDSIM or the GSA Finance Center. However, the FEDSIM COR may require the Contractor to submit a written "hardcopy" invoice with the client's certification prior to invoice payment.

G.9.6.1 INVOICE REQUIREMENTS

The Contractor shall submit simultaneous copies of the invoice to both GSA and the client POC.

If the TO has different contract types, each should be addressed separately in the invoice submission.

The final invoice is desired to be submitted within six months of project completion.

G.9.6.1.1 COST-PLUS-AWARD-FEE (CPAF) CLINs (for LABOR)

The Contractor may invoice monthly on the basis of cost incurred for the CPAF CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section B), by Contractor employee, and shall be provided for the current billing month and in total from project inception to date. The Contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

- Employee name (current and past employees)
- Employee company labor category
- Employee Alliant labor category
- Monthly and total cumulative hours worked
- Billing rate (DCMA Approved Provisional rate in support of indirect costs billed)
- Cost incurred not billed
- Current approved forward pricing rate agreement in support of indirect costs billed

All cost presentations provided by the Contractor shall also include Overhead charges, and General and Administrative charges and shall also include the Overhead and General and Administrative rates being applied.

The Government will promptly make payment of any award fee upon the submission, by the Contractor to the FEDSIM COR, of a public voucher or invoice in the amount of the total fee earned for the period evaluated. Payment may be made without issuing a TO modification if funds have been obligated for the award fee amount. The Contractor shall attach the Award Fee Determining Official (AFDO)/CO determination letter to the public voucher and/or invoice.

G.9.6.1.2 TOOLS AND/OR OTHER DIRECT COSTS (ODCs)

The Contractor may invoice monthly on the basis of cost incurred for the ODC CLIN. The invoice shall include the period of performance covered by the invoice and the CLIN number and title and Interagency Agreement (IA) number. In addition, the Contractor shall provide the following detailed information for each invoice submitted, as applicable. Spreadsheet submissions are required.

- Tools and/or ODCs purchased
- Consent to Purchase number or identifier
- Date accepted by the Government
- Associated CLIN
- Project-to-date totals by CLIN
- Cost incurred not billed

- Remaining balance of the CLIN

All cost presentations provided by the Contractor shall also include Overhead charges, General and Administrative charges, and Fee.

G.9.6.1.3 TRAVEL

The Contractor may invoice monthly on the basis of cost incurred for cost of travel comparable with the Joint Travel Regulation (JTR)/Federal Travel Regulation (FTR)/Department of State Standardized Regulations (DSSR). The invoice shall include the period of performance covered by the invoice, the CLIN number and title, and the IA number. Separate worksheets, in MS Excel format, shall be submitted for travel.

CLIN/Task Total Travel: This invoice information shall identify all cumulative travel costs billed by CLIN/Task. The current invoice period's travel details shall include separate columns and totals and include the following:

- Travel Authorization Request number or identifier, approver name, and approval date
- Current invoice period
- Names of persons traveling
- Number of travel days
- Dates of travel
- Number of days per diem charged
- Per diem rate used
- Total per diem charged
- Transportation costs
- Total charges
- Explanation of variances exceeding 10% of the approved versus actual costs
- Indirect Handling Rate

All cost presentations provided by the Contractor shall also include Overhead charges and General and Administrative charges.

G.9.7 CONTRACTOR ADMINISTRATIVE REPORTING-- APPLIES FROM BASIC ALLIANT

G.9.8 ORDER CLOSE-OUT-- APPLIES FROM BASIC ALLIANT

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract. Only those Sections listed from the Alliant Basic apply to this Task Order. In addition, the following applies:

H.1 KEY PERSONNEL

The following are the minimum personnel who shall be designated as "Key." The Contractor shall propose appropriate labor categories for these positions. The Government does not intend to dictate the composition of the ideal team to perform this TO. Therefore, the Government encourages and will evaluate additional Key Personnel as proposed by the Offeror. All Key Personnel shall have a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance.

- Program Manager
- Network Infrastructure Lead
- GCCS Lead
- Server Operation and Maintenance Lead
- Systems Engineer
- Chief Engineer – Network Management
- Network Engineer
- Lead Software Engineer
- Headquarters Information Assurance/Computer Network Defense Lead
- Enterprise Architecture Lead

The Government desires that Key Personnel be assigned for the duration of the TO.

H.1.1 PROGRAM MANAGER

The Contractor shall identify a Program Manager to serve as the Government's POC and to provide technical and administrative supervision and guidance for all Contractor personnel assigned to the TO, supervise on-going technical efforts, and manage TO performance. The Program Manager must be an employee of the prime Alliant Contractor.

It is desired that the Program Manager has the following qualifications and demonstrated experience with the following:

- The Program Manager should have and maintain Project Management Professional (PMP) certification.
- Proven expertise in the management and control of complex information systems architectures involving multiple disparate database, network, and communications subsystems.
- Experience providing technical innovations for a large scale organization, such the military or other large Government organization.
- Possess excellent written and verbal communication skills, and have experience in presenting material to senior DoD and non-DoD officials.
- Proven skills in manpower utilization, procurement, training, problem resolution, and employee relations.
- Experience in the management of cost, performance, and schedules in a Performance Based Services Contracting (PBSC) and CPAF environment.

- Staffing issues associated with Contractor personnel deployed and co-located with military personnel in an overseas location.
- C4 experience in a military headquarters or command center environment.

H.1.2 NETWORK INFRASTRUCTURE LEAD

The Contractor shall identify a Network Infrastructure Lead who will provide expertise in areas of local area and wide area IP-based networks (LAN and WAN). He/she will provide advanced technical analyses of automation challenges and problems; develop/identify technical solutions responsive to the needs of the Command; ensure information exchange and prevent duplication of effort; recommend and provide procedures, policies, and technical solutions to HQ USCENTCOM C4 challenges. He/she will participate in the planning and execution of network installations and hardware upgrades and provide a technical point of contact for all matters related to the Contractor's C4 efforts.

The Network Infrastructure Lead should be able to demonstrate experience with the following:

- Be CISCO Certified Internetwork Expert (CCIE).
- Have extensive experience managing operational networks in a high–paced, diverse environment.
- Knowledge of network analysis tools (CISCO Network Configuration Manager, CISCO Network Analysis Modules).
- WAN troubleshooting/problem determination skills (Integrated Services Digital network (ISDN), Asynchronous Transfer Mode (ATM), Synchronous Optical Network (SONET)).
- LAN troubleshooting/problem determination skills (Ethernet, Hot Standby Router Protocol (HSRP), Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP)).
- Knowledge of CISCO firewall/Virtual Private Network (VPN) equipment, Adaptive Security Appliance, NEXUS Data Center Architecture, CISCO Aggregation Service Routers (ASR), and Virtual Switching Systems (VSS).
- Knowledge of IP services (IP, Multicast, Quality of Service (QOS), Simple Network Management Protocol (SNMP)).

H.1.3 GCCS LEAD

The GCCS Task Lead is responsible for ensuring system availability and reliability for the Global Command and Control System and related systems at the HQ USCENTCOM. Systems to be maintained are on SIPRNet and all coalition networks at both rear and forward headquarters locations. The GCCS Task Lead is responsible for Command and Control program support to USCENTCOM's HQ, CFH, and AOR. The GCCS Task Lead shall prepare reports on status, outage, and performance of current systems and provides assessments of impact of new systems. The GCCS Task Lead shall manage system administration of all C2 servers and GCCS assets employed at USCENTCOM HQ and CFH.

The GCCS Task Lead should be able to demonstrate experience with the following:

- Extensive experience with GCCS and C2 systems integration in a DoD environment.

- Extensive UNIX systems administration experience.
- Experience with major platform migrations to upgrade legacy systems.
- Experience with systems architecture development.
- Extensive knowledge and planning skills in the area of system integration testing, C4 applications and networks, such as those employed by HQ USCENTCOM and as described in this PWS.
- Experience with ADP acquisition planning for major headquarters or regional site for a mid-size corporation.
- Experience with software test and evaluation plans for major releases of software or upgrade of existing hardware.
- Design and implementation of COOP sites.

H.1.4 SERVER OPERATION AND MAINTENANCE LEAD

The Contractor shall provide a Server Operation and Maintenance Lead who is responsible for systems administration, operations, maintenance, and support for all USCENTCOM networks, to include SCO, Allied, and Coalition networks. O&M shall include servers (physical and virtual), firmware, operating systems, software applications, SANs, and computer security. A robust server maintenance capability ensures that key and supporting services provided to the end user are reliable and available.

The Task Lead for Server Operation and Maintenance should be able to demonstrate experience with the following:

- Current MS Certified Solutions Expert (MCSE) certification (other certifications desired).
- Demonstrated experience providing overall enterprise level network system administration, planning, and management.
- Experience designing, managing, monitoring, and optimizing geographically dispersed networked systems.
- Experience supervising system administrators.
- Experience with project management.
- Experience performing O&M and installing upgrades.
- Experience developing, implementing, and documenting network systems.
- Experience and/or working knowledge with the following:
    - VMWare ESXi and View
    - MS Windows Server 2008, Active Directory, Exchange 2010, Outlook, System Center Configuration Manager (SCCM), and System Center Operations Manager (SCOM)

H.1.5 SYSTEMS ENGINEER

The Systems Engineer should have demonstrable experience providing overall network system optimization and operations and maintenance. The Systems Engineer should be highly technical and have extensive experience in designing, managing, monitoring, and optimizing networked systems; O&M; installing upgrades; and developing, implementing, and documenting networked systems.

The Systems Engineer should be able to demonstrate experience with the following:

- Current MCSE certification (other certifications desired).
- Extensive experience with designing, integrating, monitoring, and maintaining networked systems.
- Extensive experience with systems architecture development and design.
- Experience with remote sites operations and optimization.
- Experience with UNIX and CISCO switches.
- Experience with major platform migrations.
- Experience with software test and evaluation plans for major releases of software or upgrade of existing hardware.

H.1.6 CHIEF ENGINEER – NETWORK MANAGEMENT

The Contractor shall identify a Chief Engineer – Network Management who will provide expertise in broad areas of communications, information systems, and associated networks. He/she will participate in the planning and execution of hardware and software installations and upgrades and provide a technical POC for all matters related to the Contractor's C4 efforts. He/she will provide advanced technical analyses of automation challenges and problems; develop/identify technical solutions responsive to the needs of the Command; ensure information exchange and prevent duplication of effort; and recommend and provide procedures, policies, and technical solutions to HQ USCENTCOM C4 challenges.

The Chief Engineer – Network Management should be able to demonstrate experience with the following:

- Substantial Cisco and MS experience.
- Cisco and MS certifications desired.
- Substantial experience in system design and engineering and in developing and implementing military systems similar to the mission-critical computer and software systems at USCENTCOM Tampa HQ and the CFH.
- Data communications and messaging systems.
- Personal Computer (PC)-compatible workstations, operating systems, hardware/software interaction, and physical communications protocols.
- Excellent written and verbal communication skills, demonstrating the ability to present material to senior DoD and non-DoD officials.
- Technical oversight experience in a C4 networking environment.
- Experience as a Joint C4 Planner.

H.1.7 NETWORK ENGINEER

The Contractor shall provide a Network Engineer to design and plan network communications systems. The Network Engineer shall provide specifications and detailed schematics for network architecture. The Network Engineer shall provide specific detailed information for hardware and software selection, implementation techniques and tools for the most efficient solution to meet business needs, including present and future capacity requirements. The Network Engineer shall perform testing of network design and evaluate and report on new communications technologies to enhance capabilities of the network.

The Network Engineer should be able to demonstrate experience with the following:

- Technical expertise in all areas of network and computer hardware and software interconnection and interfacing, such as routers, multiplexers, switches, firewalls, hubs, bridges, and gateways.
- Extensive network administration experience in a CISCO environment.
- Extensive experience with designing, integrating, monitoring and maintaining interconnected networks, both LAN and WAN.
- Extensive experience with network architecture development and design.
- Extensive experience in resolving enterprise-wide issues.
- Experience with remote network operations and optimization.
- Experience with major platform migrations.
- Experience with software test and evaluation plans for major releases of software or upgrade of existing hardware.
- Knowledgeable of IPv6 technologies.
- Current CISCO Certified Network Professional (CCNP) certification required.

H.1.8 LEAD SOFTWARE ENGINEER

The Lead Software Engineer is responsible for ensuring system availability and reliability for all SQL, web, network monitoring, and portal servers supporting Tampa and CFH locations. Systems to be maintained are on SIPRNet, NIPRNet, and all coalition networks at both rear and CFH locations. The Lead Software Engineer prepares reports on status, outage, and performance of current systems and provides impact assessments of new systems. The Lead Software Engineer will be responsible for managing portal administrators, knowledge management personnel, system administrators, web developers, and database developers/architects.

The Lead Software Engineer should be able to demonstrate experience with the following:

- Experience as a team leader.
- Broad understanding of information technology principles, concepts, and techniques including software languages, design concepts, test methods, and integration practices.
- Excellent written and verbal communication skills, demonstrating the ability to present material to senior DoD and non-DoD officials. Able to communicate effectively with senior leaders and customers to clearly present technical approaches and findings.
- Experience with systems architecture development.
- Extensive knowledge and planning skills in the area of system integration testing, C4 applications and networks such as those described in this PWS.
- Experience with software test and evaluation plans for major releases of software or upgrade of existing hardware.
- Design and implement COOP program with alternate site.
- Collaborate with and assist in the development of security fixes with DISA engineers and development teams.
- Knowledgeable on web policies stated in OSD Web Site Administration, DoD Instruction 5230.29, DoD Directives 5230.9 and 5200.40.
- Responsible for implementing security and access controls.

- Ability to analyze requirements and ensure the capture of business processes.
- Experience in developing SDD for creation of KM functions within the portal environment.
- Experience providing support gathering, documenting, testing, deploying, and marketing of web content.
- Ability to develop, implement, and maintain web-based application systems.
- Experience in developing, testing, and implementing web parts for the portal.
- Highly experienced using the following program languages: C, SQL, ASP, .NET, VB and JAVA scripts.
- Understand and develop reports using SQL Reporting Tool.
- Knowledgeable on team foundation software.
- Ability to complete a comprehensive, multi-disciplinary security assessment addressing both content and technical issues at least annually on all portal/web/SQL servers.
- Knowledge of JavaScript, Cascading Style Sheets (CSS), Hypertext Preprocessor (PHP) and dynamic HyperText Markup Language (HTML); experience with .NET and team foundation.
- Experience in SharePoint, including architecture, installation, configuration, and best practices.
- Superior knowledge of current web-design trends and techniques, a strong online portfolio displaying user-centered design, and experience with web database solutions definite assets.
- Understanding of virtual environments with knowledge of clustering.

H.1.9 HEADQUARTERS INFORMATION ASSURANCE/COMPUTER NETWORK DEFENSE LEAD

The Contractor shall provide a Headquarters Information Assurance and Computer Network Defense (IA/CND) Lead to support Command Security Policy, Automated Information Systems (AIS) accreditation, risk assessments and reviews for SABI and related security evaluation activities in the support of HQ USCENTCOM C4 initiatives. The Headquarters IA/CND Lead shall serve as the IA POC for new iniatives, programs and systems, hardware and/or software being brought into the purview of the USCENTCOM site accreditation(s), HQ IA/CND policy guidance, HQ IA/CND user awareness training, and HQ IA/CND tactics, techniques and procedures for responding, preventing, and/or reacting to security alerts, incidents, or compromises.

The Headquarters IA/CND Lead should be able to demonstrate experience with the following:

- Development of Defensive Information Operations (DIO) and AIS accreditation and security policy
- In-depth understanding of incident handling and response techniques, DoD defense-in-depth architecture, DoD IA policies and mandates, NSA best security practices, and current threats and attack vectors in order maintain secure systems in support of day-to-day operations for all headquarters enclaves.
- Current Computer Information Systems Security Professional (CISSP) Certification.
- SME for key areas of IA/CND, which include security accreditation for all networks and systems IAW DoD DIACAP methodology, policy development consistent with DoD

policy and industry best security practices, incident handling and response activities and associated standard operating procedures, and user security awareness training.
- Experience performing AIS security audits.
- Experience performing a variety of network security accreditation and policy support tasks, including project management support services.
- Experience performing security design, testing, and implementation requirements of integrated networks including hardware, software and port facilities.
- Experience performing DIO accreditation/AIS security support.
- Experience performing audits for servers to include auditing reports.
- Experience performing configuration management intrusion detection, anomaly detection, and VPN systems.
- Experience performing configuration management for firewalls.
- Experience performing IA user training. Produce training material and monthly reports.
- Experience performing IA research and inspections.
- Providing guidance and implementation recommendations for security enhancements.

H.1.10 ENTERPRISE ARCHITECTURE LEAD

The Enterprise Architect Lead searches, develops/documents, and analyses enterprise, operational, and system architectures for DoD COCOM HQ, develops DoDAF-compliant views and associated data, and works with functional subject matter experts to collect and describe operational and system processes, nodes, activities, associated inputs, controls, outputs, and mechanisms. The Enterprise Architect Lead shall prepare, staff, and publish formal Command architecture documents, produce architecture development plans and reports, and conduct Strategic Architecture Branch Contractor staff actions (tasks, papers, briefings, etc.). The Enterprise Architect Lead will be responsible for researching, developing/documenting, and analyzing USCENTCOM architectures (including business/war-fighting/enterprise information environment/intelligence processes and IT) to identify mission capability gaps, overlaps, and shortfalls; determining and recommending architectural, IT, or process solutions; and researching and developing other architecture-related documents and plans.

The Enterprise Architect Lead should be able to demonstrate experience with the following:
- Understanding and experience with the DoDAF and other key DoD architecture and strategic planning instructions
- Experience producing DoDAF-compliant architectures.
- Experience with architecture tools and the MS Office Suite of software with particular emphasis on the ability to produce complex and detailed reports and presentations using these tools.
- Excellent writing and communication skills, including the ability to develop analytical documents and present oral presentations to senior management.
- Joint military experience (joint task force headquarters and/or higher)
- Experience on high-level military staff and understand DoD strategies/plans, language/terminology, and culture.
- Formal DoD architecture development education and/or equivalent architecture development experience.

H.1.11 KEY PERSONNEL SUBSTITUTION

The Contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the CO. Prior to utilizing other than personnel specified in proposals in response to a TOR, the Contractor shall notify the Government CO and the COR of the existing TO. This notification shall be no later than ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute personnel qualifications shall be equal to, or greater than, those of the personnel being substituted. If the Government CO and the COR determine that the proposed substitute personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the Contractor may be subject to default action as prescribed by FAR 52.249-6, Termination (Cost Reimbursement) or FAR 52.249-8, Default (Fixed-Price Supply and Service).

H.1.12 NON-KEY PERSONNEL

Attachment R - Non-Key Personnel Knowledge and Skills provides the desired non-key personnel knowledge and skills by task.

H.3 UNIQUE PROFESSIONAL SKILLS—APPLIES FROM BASIC ALLIANT

H.4 CONTRACTOR TRAINING

The Contractor is generally expected to maintain the professional qualifications and certifications of its personnel through on-going training. Unless an exception is specifically requested from and authorized by the Contracting Officer, the Contractor shall not directly bill the Government for any training (training costs or labor during training).

H.5 GOVERNMENT-FURNISHED PROPERTY (GFP)

The current USCENTCOM automated tools and systems shall be made available to the Contractor for use in the performance of this requirement.

The Government will provide Contractor personnel access to Government workspace including a desk, network access, telephone access, electronic mail, and access to network infrastructure and cable plant as required to perform assigned tasks.

H.5.2 GOVERNMENT-FURNISHED INFORMATION (GFI)

The Government will provide to the Contractor all available network diagrams, documentation, and all current documented policies and procedures.

H.6 PERMITS—APPLIES FROM ALLIANT BASIC

H.7 SECURITY REQUIREMENTS

Work performed as part of executing this requirement will be at the SENSITIVE BUT UNCLASSIFIED, SECRET, TOP SECRET COLLATERAL and TS/SCI levels. All Contractor personnel shall have a SECRET clearance at a minimum. This applies to all sub-Contractor

personnel as well. All Contractor personnel supporting TS/SCI networks or working at the CFH shall have TS/SCI clearances. The Government estimates that approximately 30% of the workspace at HQ USCENTCOM requires a TS/SCI clearance for access. The Contractor shall ensure that all personnel have the clearance required for the workspace(s) where they will need to work and/or a proper escort for access to the workspace(s). The Contractor shall not depend on the Government personnel for escorts for access to the workspace(s).

All SCI will be handled IAW special requirements, which will be furnished by the SSO. SCI will not be released to Contractor employees without specific release approval of the originator of the material as outlined in the appropriate governing directive. USCENTCOM is responsible for establishing the personnel security billets at the SCI level. The Contractor shall establish and maintain an access list of those employees working on this TO. A copy of the list shall be furnished to the SCI TO monitor immediately upon reassignment of personnel. USCENTCOM shall provide the Contractor with access to all areas as necessary to support this effort. SCI furnished in support of this TO remains the property of the DoD, agency, or command originator. Upon completion or termination of the TO, all SCI furnished will be returned to the direct custody of the supporting SSO, or destroyed in accordance with applicable instructions.

H.7.1 HOMELAND SECURITY PRESIDENTIAL DIRECTIVES-12 (HSPD-12)— ALLIANT BASIC APPLIES

H.7.2 INFORMATION ASSURANCE (IA)

The Contractor shall ensure that contractor personnel accessing IS have the proper and current IA certification to perform IA functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall ensure that contractor personnel meet the applicable IA certification requirements prior to assuming duties, including --

(1) DoD-approved IA workforce certification appropriate for each category and level as listed in the current version of DoD 8570.01-M.

(2) Appropriate operating system certification for IA technical positions as required by DoD 8570.01-M.

Upon request by the Government, the Contractor shall provide documentation supporting the IA certification status of personnel performing IA functions.

Contractor personnel who do not have proper and current certifications shall be denied access to DoD IS for the purpose of performing IA functions.

H.7.3 SECURITY CLEARANCES

This TO requires a minimum Secret Clearance with many tasks requiring TS Facility/Personnel Clearances. All Contractor personnel working in a USCENTCOM-designated space are required to:

1. Have undergone a Single Scope Background Investigation (SSBI) or Single Scope Background Investigation - Periodic Review (SSBI-PR) within the last five years that was favorably adjudicated.
2. Have no break greater than 24 months in military service, Federal civilian employment, or access to classified information under the Industrial Security Program.
3. Possess a current Top Secret security determination for certain tasks (to be specified in the solicitation).
4. Possess an SCI determination reflected in Joint Personnel Adjudication System (JPAS) for certain tasks (to be specified in the solicitation).

*** Tasks marked with an asterisk will require a TS/SCI clearance for some but not all personnel working on that task.**

Task	Description	Required Security Clearance
5.2	C4 Systems Support	
5.2.1	C3 Systems Support	
5.2.1.1	Management of HQ Systems Infrastructure	TS/SCI
5.2.1.2	Voice Services	TS/SCI
5.2.1.3	Patch and Test Facility (PTF) Support	TS/SCI
5.2.1.4	Cable Plant Support	TS/SCI
5.2.2	Enterprise Network Services Support	
5.2.2.1	Communications Support	TS/SCI
5.2.2.2	GCCS Support	TS/SCI*
5.2.2.3	End-User Information Technology Support	TS/SCI
5.2.2.4	Server Maintenance Support	TS/SCI*
5.2.2.5	Wireless Support	S
5.2.3	Operations Support	
5.2.3.1	**Visual Information Systems**	**TS/SCI**
5.2.3.2	**Security Cooperation Offices (SCO) Support**	**TS/SCI**
5.2.4	Customer Support Operations	S
5.2.5	Commander Communications Support	TS/SCI
5.2.6	**HQ User Training**	**S**
5.3	Theater Network Operations (NetOps) Support	
5.3.1	Level 0 Fault Monitoring, Identification, Resolution	S
5.3.2	Level 1 Current Operations	S
5.3.3	Information Assurance – CND	TS/SCI*
5.4	Engineering Support	
5.4.1	Project Management	TS/SCI*
5.4.2	Engineering Support	
5.4.2.1	Engineering and Technology Support	TS/SCI*
5.4.2.2	Engineering Design Analysis	S
5.4.2.3	Coalition Network Architecture Engineering	S
5.2.3.4	Configuration and Enterprise License Management	S
5.4.2.5	Engineering Monitoring Tools Support	S
5.4.2.6	Change Management	S
5.4.3	Engineering, Test, Analysis and Integration Lab	S
5.4.4	Software Engineering Support	TS/SCI*

5.5	Cyber Support	
5.5.1	Headquarters Network Defense	TS/SCI
5.5.2	Theater Cyber Initiatives	TS/SCI
5.5.3	Cyber Certification and Accreditation	S
5.6	Programs and Architectures Support	
5.6.1	Programs and Architectures	
5.6.1.1	Program Planning and Development Support	TS/SCI
5.6.1.2	Multi-National Information Sharing (MNIS) Support	TS/SCI*
5.6.2	Chief Information Officer (CIO) Support	S
5.6.3	Architectures Support	
5.6.3.1	Architectures Support	TS/SCI
5.6.3.2	Solution Architecture and JCIDS Analysis Support	S
5.6.4	Knowledge Management (OPTIONAL TASK)	TS/SCI
5.7	Resource Management Support	
5.7.1	Records Management Support	TS/SCI*
5.7.2	Asset Management Support	TS/SCI

In order to report to USCENTCOM-designated spaces for the first day of employment, Contractor personnel must possess a current TS clearance with an SCI determination reflected in JPAS and be formally nominated by their company's security office to be indoctrinated into SCI programs.

Contractors must ensure that all proposed personnel possess the required security clearances (or are TSC/SCI Eligible) at the time of proposal.

H.7.3.1 Additional Security Requirements

The Contractor shall ensure their personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program. The Contractor shall meet the applicable information assurance certification requirements including:

- DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M
- Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

The table below provides that DOD 8570 requirements for personnel working on specific tasks.

Task	DoD 8570 Certification
C.5.2.1.1 Management of HQ Systems Infrastructure	All staff proposed must have DoD 8570 IAT-2 certification
C.5.2.1.2 Voice Services	All staff proposed must have at least DoD 8570 IAT-1 and at least 75% proposed must have DoD 8570 IAT-2 certification
C.5.2.1.3 Patch and Test Facility (PTF) Support	All staff proposed must have DoD 8570 IAT-1 certification
C.5.2.2.1 Communications Center	All staff proposed must have DoD 8570 IAT-2 certification
C.5.2.2.2 GCCS Support	All staff proposed must have DoD 8570 IAT-2 certification
C.5.2.2.3 End-User Information Technology (IT) System Support	All staff proposed must have DoD 8570 IAT-2 certification
C.5.2.2.4 Server Maintenance Support	All staff proposed must have DoD 8570 IAT-2 certification
C.5.2.2.5 Wireless Communications	All staff proposed must have DoD 8570 IAT-2 certification
C.5.2.3.1 Visual Information Systems	50% of the staff proposed must have DoD 8570 IAT-2 certification
C.5.2.3.2 Security Cooperation Offices (SCO) Support	All staff proposed must have DoD 8570 IAT-2 certification
C.5.2.4 Customer Support Operations	All staff proposed must have at least DoD 8570 IAT-1 and at least 50% proposed must have DoD 8570 IAM-1 certification
C.5.2.5 Commander Communications Support	All staff proposed must have DoD 8570 IAT-3 certification
C.5.3.1 Level 0 Fault Monitoring, Identification, Resolution	50% of the staff proposed must have DoD 8570 IAT-2 certification
C.5.3.2 Level 1 Current Operations	50% of the staff proposed must have DoD 8570 IAT-2 certification
C.5.3.3 Information Assurance – CND	All staff proposed must have DoD 8570 IAM-2 certification

H.8 LOGISTICAL SUPPORT PRIVILEGES

Status of Forces Agreements (SOFAs) for foreign jurisdictions will apply and will be processed for foreign tax exemption purposes. At the discretion of the Military Theatre Commander, the Government may provide, but is not limited to, use of the following:

(a) Military or other U.S. Government Clubs, exchanges, or other non-appropriated fund organizations

(b) Military or other U.S. Government commissary stores

(c) Military or other U.S. Government postal facilities

(d) Utilities and services in accordance with priorities, rates, or tariffs established by military or other U.S. Government agencies

(e) Military Payment Certificate (MPC), where applicable

(f) Military or other U.S. Government banking facilities

(g) Military or other U.S. Government provided telephones, lines, and services with direct dialing capability and access to the DSN

The precedence of usage shall be coincident with the urgency of the requirement and in accordance with Government and Military regulations. A detailed description of the Contractor logistics support provided by the Government can be found at http://www.BTA.Mil/products/spot.html.

H.9 ORGANIZATIONAL CONFLICT OF INTEREST AND NON-DISCLOSURE REQUIREMENTS

H.9.1 ORGANIZATIONAL CONFLICT OF INTEREST

If the Contractor has in the past, is currently providing support or anticipates providing support to USCENTCOM that creates or represents an actual or potential organizational conflict of interest (OCI), the Contractor shall immediately disclose this actual or potential OCI in accordance with FAR Subpart 9.5. The Contractor is also required to complete and sign an Organizational Conflict of Interest Statement in which the Contractor (and any subcontractors, consultants, or teaming partners) agrees to disclose information concerning the actual or potential conflict with any proposal for any solicitation relating to any work in the TO. All actual or potential OCI situations shall be identified and addressed in accordance with FAR Subpart 9.5.

H.9.2 NON-DISCLOSURE REQUIREMENTS

If the contractor acts on behalf of, or provides advice with respect to any phase of an agency procurement, as defined in FAR 3.104-4, then the contractor shall execute and submit a Corporate Non-Disclosure Agreement (NDA) Form (Section J, Attachment E) and ensure that all its personnel (to include subcontractors, teaming partners, and consultants) who will be personally and substantially involved in the performance of the TO:

a. Are listed on a signed Addendum to Corporate Non-Disclosure Agreement (NDA) Form (Section J, Attachment E) prior to the commencement of any work on the TO, and

b. Are instructed in the FAR 3.104 requirements for disclosure, protection, and marking of contractor bid or proposal information, or source selection information.

All proposed replacement contractor personnel also must be listed on a signed Addendum to Corporate NDA and be instructed in the requirements of FAR 3.104. Any information provided by contractors in the performance of this TO or obtained by the Government is only to be used in the performance of the TO. The contractor shall put in place appropriate procedures for the protection of such information and shall be liable to the Government for any misuse or unauthorized disclosure of such information by its personnel, as defined above.

H.10 INCORPORATION OF SUBCONTRACTING PLAN—ALLIANT BASIC APPLIES

H.11 GOALS FOR SUBCONTRACTING—ALLIANT BASIC APPLIES

H.12 ELECTRONIC PRODUCTS ENVIRONMENTAL ASSESSMENT TOOL—ALLIANT BASIC APPLIES

H.14 SECTION 508 COMPLIANCE REQUIREMENTS

Unless the Government invokes an exemption, all Electronic and Information Technology (EIT) products and services proposed shall fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, 29 United States Code (U.S.C.) 794d, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 Code of Federal Regulations (CFR) 1194. The Contractor shall identify all EIT products and services proposed, identify the technical standards applicable to all products and services proposed and state the degree of compliance with the applicable standards. Additionally, the Contractor must clearly indicate where the information pertaining to Section 508 compliance can be found (e.g., Vendor's or other exact web page location). The Contractor must ensure that the list is easily accessible by typical users beginning at time of award.

H.15 INSURANCE—ALLIANT BASIC APPLIES

H.16 COST ACCOUNTING SYSTEM - ALLIANT BASIC APPLIES

H.17 COST ACCOUNTING STANDARDS - ALLIANT BASIC APPLIES

H.18 PURCHASING SYSTEMS

The objective of a Contractor purchasing system assessment is to evaluate the efficiency and effectiveness with which the Contractor spends Government funds and complies with Government policy with subcontracting.

Prior to the award of a TO the CO shall verify the validity of the Contractor's purchasing system. Thereafter, the Contractor is required to certify to the CO no later than 30 calendar days prior to the exercise of any options the validity of their purchasing system. Additionally, if reviews are conducted of the purchasing system after the exercise of the option, the Contractor shall provide the results of the review to the CO within 10 workdays from the date the results are known to the Contractor.

H.20 YEAR 2000 WARRANTY – COMMERCIAL/NON-COMMERCIAL SUPPLY ITEMS –ALLIANT BASIC APPLIES

H.23 TRAVEL

H.23.1 TRAVEL REGULATIONS

Contractor costs for travel will be reimbursed at the limits set in the following regulations (see FAR 31.205-46):

(1) Federal Travel Regulations (FTR) - prescribed by the GSA, for travel in the contiguous U.S.

(2) Joint Travel Regulations (JTR), Volume 2, Department of Defense (DoD) Civilian Personnel, Appendix A - prescribed by the DoD, for travel in Alaska, Hawaii, and outlying areas of the U.S.

(3) Department of State Standardized Regulations (DSSR) (Government Civilians, Foreign Areas), Section 925, "Maximum Travel Per Diem Allowances for Foreign Areas" - prescribed by the Department of State, for travel in areas not covered in the FTR or JTR.

H.23.2 TRAVEL AUTHORIZATION REQUESTS

Before undertaking travel to any Government site or any other site in performance of this Contract, the Contractor shall have this travel approved by, and coordinated with, the FEDSIM COR. Notification shall include, at a minimum, the number of persons in the party, traveler name, destination, duration of stay, purpose, and estimated cost. Prior to any long distance travel, the Contractor shall prepare a Travel Authorization Request for Government review and approval. Long distance travel will be reimbursed for cost of travel comparable with the FTR, JTR, and the DSSR.

Requests for travel approval shall:

- Be prepared in a legible manner.
- Include a description of the travel proposed including a statement as to purpose.
- Be summarized by traveler.
- Identify the TO number.
- Identify the CLIN and Interagency Agreement account associated with the travel.
- Be submitted in advance of the travel with sufficient time to permit review and approval.

The Contractor shall use only the minimum number of travelers and rental cars needed to accomplish the task(s). Travel shall be scheduled during normal duty hours whenever possible.

H.24 TOOLS AND ODCs

The Government may require the Contractor to purchase hardware, software, and related supplies critical and related to the services being acquired under the TO. Such requirements will be identified at the time a TOR is issued or may be identified during the course of a TO by the Government or the Contractor. If the Contractor initiates a purchase within the scope of this TO and the prime Contractor has an approved purchasing system, the Contractor shall submit to the FEDSIM COR a Request to Initiate Purchase (RIP). If the prime Contractor does not have an approved purchasing system, the Contractor shall submit to the CO a Consent to Purchase (CTP). The RIP and CTP shall include the purpose, specific items, estimated cost, cost comparison, and rationale. The Contractor shall not make any purchases without an approved RIP from the COR or an approved CTP from the CO.

H.25 TRANSFER OF HARDWARE/SOFTWARE MAINTENANCE AGREEMENTS

If the Offeror proposes to provide any commercial computer software ("Commercial Software") as part of its proposed solution in response to this Solicitation, the Offeror shall ensure that any software license agreement ("License Agreement") associated with such Commercial Software and intended to bind the Government complies with the FAR clause at 12.212(a), which

provides, in relevant part, that commercial computer software and documentation shall be acquired under licenses customarily provided to the public "to the extent such licenses are consistent with Federal law." The most common examples of areas of non-compliance are set forth in the following table, which is provided for information purposes only and does not constitute an exhaustive list.

The requirement to propose compliant License Agreements shall apply regardless of whether the original rights holder to the Commercial Software ("Licensor") is the Offeror, its subcontractor, or a third party, in the case of third-party software embedded or provided with the Commercial Software. Further, this requirement shall apply regardless of the format or title of the License Agreement (i.e., whether entitled "Software License Agreement," "End User License Agreement," "Terms of Service," or otherwise and whether presented in hard copy or in a clickwrap or other electronic format). For the avoidance of doubt, this may require the Offeror to negotiate with its Licensors and to obtain a revised version of the License Agreement. License Agreements incorporated into a company's existing Schedule 70 or other Government contract are not exempt from this requirement.

If proposing Commercial Software, the Offeror shall include a statement in its proposal certifying that all applicable License Agreements will comply with the requirement of this Section H (actual License Agreements need not be submitted prior to award). Failure to certify compliance will render the proposal ineligible for award, and non-compliance identified after award may entitle the Government to terminate the contract and seek any or all available remedies for breach of contract.

Commercial Terms*	Legal Restriction	Action**
Contract Formation and Modification	Under FAR 1.601(a), in an acquisition involving the use of appropriated funds, an agreement binding on the Government may only be entered into by a duly warranted CO in writing. Under FAR 43.102, the same requirement applies to contract modifications affecting the rights of the parties.	Any provisions purporting to form a contract binding on the U.S. Government by any other means (e.g., use, download, click through terms, etc.) must be deleted. The same applies to provisions allowing for License Agreement terms to be changed unilaterally by the Licensor.

Commercial Terms*	Legal Restriction	Action**
Patent or Other Type of Intellectual Property Indemnity – sellers of products or services often provide that in the event of claim or litigation alleging infringement of patent rights asserted by some third party that the seller will indemnify the buyer, provided that the buyer provide notice of the claim or litigation, and that the seller assume control of the litigation and any proposed settlement.	Under the authority of 28 U.S.C. § 516, only the Attorney General, acting by and through the attorneys of the U.S. Department of Justice, may represent the U.S. Government in litigation.	The patent or other type of intellectual property indemnity clause remains in effect, but any undertaking to "defend" the Government or any requirement that the seller control litigation and/or any proposed settlement is to be deleted.
General Indemnity – sellers of products or services provide that in the event of any litigation arising from the buyers use of the product or service that buyer will indemnify seller's litigation costs and damages (if any).	Agreements to pay the attorney fees of a private party require a statutory waiver of sovereign immunity. Agreements to pay some indeterminate amount of money in the future violate the restrictions of the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1) and the Adequacy of Appropriations Act, 41 U.S.C. §11.	General Indemnity clauses must be removed from the License Agreement.
Arbitration of Disputes – sellers of products or services provide that any disputes with buyer must be resolved through binding arbitration without recourse to litigation in state or federal courts.	Federal Agencies are not allowed to use binding arbitration unless the head of the agency has promulgated guidance through administrative rulemaking on the use of binding arbitration. *See* 5 U.S.C. § 575. At the time of this Solicitation release, GSA has not done so.	Binding Arbitration clauses must be removed from the License Agreement.

Commercial Terms*	Legal Restriction	Action**
Venue, Jurisdiction and Choice of Law – sellers of products or services provide that jurisdiction of any dispute will be in a particular state, federal or foreign court or that particular state or foreign law will govern.	Litigation where the U.S. Government is a defendant must be heard either in U.S. District Court (28 U.S.C. § 1346) or the U.S. Court of Federal Claims (28 U.S.C. §1491). The U.S. Government, as the sovereign, does not contract under state or foreign law. Depending on the subject matter of the dispute, the Contract Disputes Act or other applicable law will govern.	Clauses claiming that disputes will only be heard in state court will be revised to allow disputes in Federal court. Choice of law clauses must be deleted.
Equitable Remedies – sellers of products or services provide that in the event of a dispute concerning patent or copyright infringement that the end user agree that an injunction is appropriate.	The only remedy provided for copyright or patent infringement against the U.S. Government is monetary damages. *See* 28 U.S.C. § 1498.	Equitable remedy clauses must be removed.
Negative Options – sellers of products or services provide that option periods will automatically be exercised unless affirmative action is taken by the buyer to not exercise the option.	Agreements to pay money in advance of appropriations violate the restrictions of the Anti-Deficiency Act, 31 U.S.C. § 1341(a)(1) and the Adequacy of Appropriations Act, 41 U.S.C. §11.	Negative option clauses must be removed.

Commercial Terms*	Legal Restriction	Action**
Limitation of Liability	Various (see next column)	Limitation of liability clauses may be included in accordance with the Licensor's standard commercial practices, except that such clauses may not operate to impair or prejudice the U.S. Government's right (a) to recover for fraud or crimes arising out of or relating to this TO under any Federal fraud statute, including without limitation the False Claims Act (31 U.S.C. §§3729 through 3733), or (b) to express remedies provided under any FAR, GSAR or master Alliant contract clauses incorporated into this TO.
Integration/Order of Precedence Clauses		Any provisions purporting to invalidate or supersede the terms of the Government TO resulting from this Solicitation (such provisions are frequently found in "entire agreement" clauses) must be removed from the License Agreement.

* The following standard commercial terms are deemed non-compliant within the meaning of this clause.

** The License Agreement will be deemed compliant when the action specified in this column is successfully implemented.

H.26 AWARD FEE

The Award Fee Determination Plan is contained in Section J Attachment B.

H.26.1 ESTABLISHMENT AND DETERMINATION OF AWARD FEE

The award fee dollar pool will be established on execution of the TO. The Government reserves the right to adjust these amounts to reflect any change in the Estimated Cost for the anticipated five-year period of this TO. The amount of Award Fee is established at award and cannot exceed 8% over the life of the order.

The Government will, at the conclusion of each specified evaluation period(s), evaluate the Contractor's performance for a determination of award fee earned. The Contractor agrees that the determination as to the amount of the award fee earned will be made by the Government AFDO and such determination is binding on both parties and shall not be subject to the "Disputes" clause or to any board or court.

The evaluation of Contractor performance will be in accordance with the Award Fee Determination Plan (AFDP) (Section H.26.2). The Government will promptly advise the Contractor in writing of the determination and reasons why the award fee was not earned. The Contractor may submit a self-evaluation of performance for each period under consideration. While it is recognized that the basis for the determination of the fee will be the evaluation by the Government, any self-evaluation which is received within 15 workdays after the end of the period being evaluated may be given consideration as deemed appropriate by the Award Fee Evaluation Board (AFEB). Any cost associated with the development and presentation of a self-evaluation will not be allowed as a direct cost to this TO.

H.26.2 AWARD FEE DETERMINATION PLAN (AFDP)

An AFDP will be established by the Government, in consultation with the Contractor, based on the objectives and concerns provided in the TO request and the Contractor-provided solutions. The AFDP will include the criteria used to evaluate each area and the percentage of award fee available for each area. The initial plan will be finalized NLT 15 workdays after award date.

The AFDP may be revised unilaterally by the Government at any time during the period of performance. The Government will make every attempt to provide changes to the Contractor 15 workdays prior to the start of the evaluation period to which the change will apply. The AFDP may be re-evaluated each evaluation period with input from the Contractor.

The Government may, at its option, unilaterally revise the plan to include metrics gathered from the re-evaluation to be applied in future award fee periods.

H.26.4 DISTRIBUTION OF AWARD FEE

Award Fee will be distributed in accordance with the AFDO determination and the AFDP (Section J, Attachment B).

If the Government initiates any action that impacts the contractual scope of work and/or schedule pursuant to the "changes" clause or other pertinent provisions of the TO, the maximum award fee available for payment for any evaluation periods impacted will be modified as negotiated between the parties.

H.27 CONTRACTOR IDENTIFICATION

As stated in 48 CFR 211.106, Purchase Descriptions for Service Contracts, Contractor personnel shall identify themselves as Contractor personnel by introducing themselves or being introduced as Contractor personnel and by displaying distinguishing badges or other visible identification for meetings with Government personnel. Contractor personnel shall appropriately identify themselves as Contractor employees in telephone conversations and in formal and informal written correspondence.

H.28 INTELLECTUAL PROPERTY RIGHTS

The existence of any patent, patent application or other intellectual property right that encumbers any deliverable must be disclosed in writing on the cover letter that accompanies the delivery. If no such disclosures are provided, the data rights provisions in DFAR 252.227-2021 apply.

H.29 REGULATORY GUIDANCE

The Contractor shall perform the requirements of this TO in accordance with the Regulations and Publications provided in Section J, Attachment N.

NOTE: The Section numbers in this TO correspond to the Section numbers in the Alliant Contract. Only those Sections listed from the Alliant Basic apply to this Task Order. In addition, the following applies:

I.1 FAR 52.252-2 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at these addresses:

https://www.acquisition.gov/far/index.html
https://www.acquisition.gov/gsam/gsam.html

CLAUSE NO.	TITLE	DATE
52.202-1	DEFINITIONS	JUL 2004
52.203-3	GRATUITIES	APR 1984
52.203-5	COVENANT AGAINST CONTINGENT FEES	APR 1984
52.203-6	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT	SEP 2006
52.203-7	ANTI-KICKBACK PROCEDURES	OCT 2010
52.203-8	CANCELLATION, RESCISSION, AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY	JAN 1997
52.203-10	PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY	JAN 1997
52.203-12	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS	OCT 2010
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT	APR 2010
52.204-2	SECURITY REQUIREMENTS	AUG 1996
52.204-4	PRINTED OR COPIED DOUBLE-SIDED ON RECYCLED PAPER	AUG 2000
52.204-7	CENTRAL CONTRACTOR REGISTRATION	APR 2008
52.204-9	PERSONAL IDENTITY VERIFICATION OF CONTRACTOR PERSONNEL	SEP 2007
52.204-10	REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT AWARDS	JUL 2010
52.207-3	RIGHT OF FIRST REFUSAL OF EMPLOYMENT	MAY 2006
52.208-9	CONTRACTOR USE OF MANDATORY SOURCES OF SUPPLY OR SERVICES	OCT 2008
52.209-6	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT	SEP 2006
52.214-35	SUBMISSION OF OFFERS IN U.S. CURRENCY	APR 1991
52.215-2	AUDIT AND RECORDS —NEGOTIATION	MAR 2009

CLAUSE NO.	TITLE	DATE
52.215-8	ORDER OF PRECEDENCE – UNIFORM CONTRACT FORMAT	OCT 1997
52.215-10	PRICE REDUCTION FOR DEFECTIVE COST OR PRICING DATA	OCT 2010
52.215-11	PRICE REDUCTION FOR DEFECTIVE COST OR PRICING DATA – MODIFICATIONS	OCT 2010
52.215-12	SUBCONTRACTOR COST OR PRICING DATA	OCT 2010
52.215-13	SUBCONTRACTOR COST OR PRICING DATA – MODIFICATIONS	OCT 2010
52.215-14	INTEGRITY OF UNIT PRICES	OCT 2010
52.215-14	ALTERNATE I	OCT 1997
52.215-15	PENSION ADJUSTMENTS AND ASSET REVERSIONS	OCT 2010
52.215-16	FACILITIES CAPITAL COST OF MONEY	JUN 2003
52.215-17	WAIVER OF FACILITIES CAPITAL COST OF MONEY	OCT 1997
52.215-18	REVERSION OR ADJUSTMENT OF PLANS FOR POSTRETIREMENT BENEFITS (PRB) OTHER THAN PENSIONS	JUL 2005
52.215-21	REQUIREMENTS FOR COST OR PRICING DATA OR INFORMATION OTHER THAN COST OR PRICING DATA-MODIFICATIONS	OCT 2010
52.215.21	ALTERNATE I	OCT 2010
52.216-7*	ALLOWABLE COST AND PAYMENT FILLIN "30TH"	DEC 2002
52.217-8*	OPTION TO EXTEND SERVICES "within 60 days"	NOV 1999
52.219-8	UTILIZATION OF SMALL BUSINESS CONCERNS	MAY 2004
52.219-9	SMALL BUSINESS SUBCONTRACTING PLAN	APR 2008
52.219-9	ALTERNATE II	OCT 2001
52.219-16	LIQUIDATED DAMAGES – SUBCONTRACTING PLAN	JAN 1999
52.222-2*	PAYMENT FOR OVERTIME PREMIUMS FILLIN "$0.00"	JUL 1990
52.222-3	CONVICT LABOR	JUN 2003
52.222-21	PROHIBITION OF SEGREGATED FACILITIES	FEB 1999
52.222-26	EQUAL OPPORTUNITY	MAR 2007
52.222-29	NOTIFICATION OF VISA DENIAL	JUN 2003
52.222-35	EQUAL OPPORTUNITY FOR SPECIAL DISABLED VETERANS, VETERANS OF THE VIETNAM ERA, AND OTHER ELIGIBLE VETERANS	SEP 2006
52.222-36	ALTERNATE I	JUN 1998

CLAUSE NO.	TITLE	DATE
52.222-37	EMPLOYMENT REPORTS ON SPECIAL DISABLED VETERANS, VETERANS OF THE VIETNAM ERA, AND OTHER ELIGIBLE VETERANS	SEP 2006
52.222-50	COMBATING TRAFFICKING IN PERSONS	FEB 2009
52.222-54	EMPLOYMENT ELIGIBILITY VERIFICATION	JAN 2009
52.223-5	POLLUTION PREVENTION AND RIGHT-TO-KNOW INFORMATION. ALTERNATE I	AUG 2003
52.223-6	DRUG-FREE WORKPLACE	MAY 2001
52.225-8	DUTY-FREE ENTRY	FEB 2000
52.225-13	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES	JUN 2008
52.225-14	INCONSISTENCY BETWEEN ENGLISH VERSION AND TRANSLATION OF CONTRACT	FEB 2000
52.225-19	CONTRACTOR PERSONNEL IN A DESIGNATED OPERATIONAL AREA OR SUPPORTING A DIPLOMATIC OR CONSULAR MISSION OUTSIDE THE UNITED STATES	MAR 2008
52.228-3	WORKERS' COMPENSATION INSURANCE (DEFENSE BASE ACT)	APR 1984
52.228-4	WORKERS' COMPENSATION AND WAR-HAZARD INSURANCE OVERSEAS	APR 1984
52.228-7	INSURANCE – LIABILITY TO THIRD PERSONS	MAR 1996
52.229-3	FEDERAL, STATE, AND LOCAL TAXES	APR 2003
52.229-4	FEDERAL, STATE, AND LOCAL TAXES (STATE AND LOCAL ADJUSTMENTS)	APR 2003
52.229-8*	TAXES – FOREIGN COST-REIMBURSEMENT CONTRACTS FILLIN "NONE"	MAR 1990
52.230-2	COST ACCOUNTING STANDARDS	OCT 2010
52.230-3	DISCLOSURE AND CONSISTENCY OF COST ACCOUNTING PRACTICES	OCT 2008
52.230-6	ADMINISTRATION OF COST ACCOUNTING STANDARDS	JUN 2010
52.232-9	LIMITATION ON WITHHOLDING OF PAYMENTS	APR 1984
52.232-17	INTEREST	OCT 2010
52.232-18	AVAILABILITY OF FUNDS	APR 1984
52.232-20	LIMITATION OF COSTS	APR 1984
52.232-22	LIMITATION OF FUNDS	APR 1984
52.232-23	ASSIGNMENT OF CLAIMS	JAN 1986
52.232-25	PROMPT PAYMENT	OCT 2008
52.232-25	ALTERNATE I	FEB 2002
52.232-33	PAYMENT BY ELECTRONIC FUNDS TRANSFER-CENTRAL CONTRACTOR REGISTRATION	OCT 2003

CLAUSE NO.	TITLE	DATE
52.233-1	DISPUTES	JUL 2002
52.233-1	ALTERNATE I	DEC 1991
52.233-3	PROTEST AFTER AWARD	AUG 1996
52.233-3	ALTERNATE I	JUN 1985
52.237-2	PROTECTION OF GOVERNMENT BUILDINGS, EQUIPMENT, AND VEGETATION	APR 1984
52.237-3	CONTINUITY OF SERVICES	JAN 1991
52.237-10	IDENTIFICATION OF UNCOMPENSATED OVERTIME	OCT 1997
52.239-1	PRIVACY OR SECURITY SAFEGUARDS	AUG 1996
52.242-1	NOTICE OF INTENT TO DISALLOW COSTS	APR 1984
52.242-3	PENALTIES FOR UNALLOWABLE COSTS	MAY 2001
52.242-4	CERTIFICATION OF FINAL INDIRECT COSTS	JAN 1997
52.242-13	BANKRUPTCY	JUL 1995
52.243-2	CHANGES – COST REIMBURSEMENT	AUG 1987
52.243-2	ALTERNATE II	APR 1984
52.244-2*	SUBCONTRACTS FILLIN “NO SPECIFIC CONSENT REQUIRED”	JUN 2007
52.244-5	COMPETITION IN SUBCONTRACTING	DEC 1996
52.245-1	GOVERNMENT PROPERTY	JUN 2007
52.245-2	GOVERNMENT PROPERTY INSTALLATION OPERATION SERVICES	JUN 2007
52.245-9	USE AND CHARGES	JUN 2007
52.246-25	LIMITATION OF LIABILITY – SERVICES	FEB 1997
52.249-2	TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (FIXED-PRICE)	MAY 2004
52.249-6	TERMINATION (COST-REIMBURSEMENT)	MAY 2004
52.249-14	EXCUSABLE DELAYS	APR 1984
52.250-5	SAFETY ACT – EQUITABLE ADJUSTMENT	FEB 2009
52.251-1	GOVERNMENT SUPPLY SOURCES	APR 1984
52.251-2	INTERAGENCY FLEET MANAGEMENT SYSTEM VEHICLES AND RELATED SERVICES	JAN 1991
52.253-1	COMPUTER GENERATED FORMS	JAN 1991

(Note: Clause numbers followed by an asterisk (*) require fill-ins by the OCO if determined applicable and incorporated into the Order.)

I.2 FAR 52.209-9 ALTERNATE I

(a)(1) The Contractor shall update the information in the Federal Awardee Performance and Integrity Information System (FAPIIS) on a semi-annual basis, throughout the life of the contract, by posting the required information in the Central Contractor Registration database at http://www.ccr.gov.

(a)(2) At the first semi-annual update on or after April 15, 2011, the Contractor shall post again any required information that the Contractor posted prior to April 15, 2011.
(b)(1) The Contractor will receive notification when the Government posts new information to the Contractor's record.
(2) The Contractor will have an opportunity to post comments regarding information that has been posted by the Government. The comments will be retained as long as the associated information is retained, i.e., for a total period of 6 years. Contractor comments will remain a part of the record unless the Contractor revises them.
(3)(i) Public requests for system information posted prior to April 15, 2011, will be handled under Freedom of Information Act procedures, including, where appropriate, procedures promulgated under E.O. 12600.
(ii) As required by section 3010 of Public Law 111-212, all information posted in FAPIIS on or after April 15, 2011, except past performance reviews, will be publicly available.

I.3 FAR 52.215-19 NOTIFICATION OF OWNERSHIP CHANGES (OCT 1997)

(a) The Contractor shall make the following notifications in writing:

(1) When the Contractor becomes aware that a change in its ownership has occurred, or is certain to occur, that could result in changes in the valuation of its capitalized assets in the accounting records, the Contractor shall notify the ACO within 30 days.

(2) The Contractor shall also notify the ACO within 30 days whenever changes to asset valuations or any other cost changes have occurred or are certain to occur as a result of a change in ownership.

(b) The Contractor shall--

(1) Maintain current, accurate, and complete inventory records of assets and their costs;

(2) Provide the ACO or designated representative ready access to the records upon request;

(3) Ensure that all individual and grouped assets, their capitalized values, accumulated depreciation or amortization, and remaining useful lives are identified accurately before and after each of the Contractor's ownership changes; and

(4) Retain and continue to maintain depreciation and amortization schedules based on the asset records maintained before each Contractor ownership change.

(c) The Contractor shall include the substance of this clause in all subcontracts under this contract that meet the applicability requirement of FAR 15.408(k).

I.4 FAR 52.216-18 ORDERING (OCT 1995)

(a) Any supplies and services to be furnished under this contract shall be ordered by issuance of delivery orders or task orders by the individuals or activities designated in the Schedule. Such orders may be issued in accordance with Section F.3.

(b) All delivery orders or task orders are subject to the terms and conditions of this contract. In the event of conflict between a delivery order or task order and this contract, this contract shall control.

(c) If mailed, a delivery order or task order is considered "issued" when the Government deposits the order in the mail. Orders may be issued orally, by facsimile, or by electronic commerce methods only if authorized by the Schedule.

I.6 FAR 52.216-19 ORDER LIMITATIONS (OCT 1995)

(a) *Minimum order*. When the Government requires supplies or services covered by this contract in an amount of less than $1 Million the Government is not obligated to purchase, nor is the Contractor obligated to furnish, those supplies or services under the contract.

(b) *Maximum order*. The Contractor is not obligated to honor:

(1) Any order for a single item in excess of $1 Billion;

(2) Any order for a combination of items in excess of $1 Billion;

(3) A series of orders from the same ordering office within 10 days that together call for quantities exceeding the limitation in subparagraph (1) or (2) above.

(c) If this is a requirements contract (*i.e.,* includes the Requirements clause at subsection 52.216-21 of the Federal Acquisition Regulation (FAR), the Government is not required to order a part of any one requirement from the Contractor if that requirement exceeds the maximum-order limitations in paragraph (b) of this section.

(d) Notwithstanding paragraphs (b) and (c) of this section, the Contractor shall honor any order exceeding the maximum order limitations in paragraph (b), unless that order (or orders) is returned to the ordering office within three (3) work days after issuance, with written notice stating the Contractor's intent not to ship the item (or items) called for and the reasons. Upon receiving this notice, the Government may acquire the supplies or services from another source.

I.7 FAR 52.216-22 INDEFINITE QUANTITY (OCT 1995)

(a) This is an indefinite-quantity contract for the supplies or services specified, and effective for the period stated, in the Schedule. The quantities of supplies and services specified in the Schedule are estimates only and are not purchased by this contract.

(b) Delivery or performance shall be made only as authorized by orders issued in accordance with the Ordering clause. The Contractor shall furnish to the Government, when and if ordered, the supplies or services specified in the Schedule up to and including the quantity designated in the Schedule as the "maximum." The Government shall order at least the quantity of supplies or services designated in the Schedule as the "minimum."

(c) Except for any limitations on quantities in the Order Limitations clause or in the Schedule, there is no limit on the number of orders that may be issued. The Government may issue orders requiring delivery to multiple destinations or performance at multiple locations.

(d) Any order issued during the effective period of this contract and not completed within that period shall be completed by the Contractor within the time specified in the order. The contract shall govern the Contractor's and Government's rights and obligations with respect to that order to the same extent as if the order were completed during the contract's effective period; provided, that the Contractor shall not be required to make any deliveries under this contract after 60 months following the expiration of the basic contract ordering period.

I.8 FAR 52.217-9 OPTION TO EXTEND THE TERM OF THE CONTRACT (MAR 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days of the expiration of the contract; provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 60 days before the contract expires. The preliminary notice does not commit the Government to an extension.

(b) If the Government exercises this option, the extended contract shall be considered to include this option clause.

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 10 years.

I.9 FAR 52.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any GSAM (48 CFR Chapter 5) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

I.10 GENERAL SERVICES ADMINISTRATION ACQUISITION MANUAL (GSAM), INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

GSAM website: https://www.acquisition.gov/gsam/gsam.html

Clause No	Clause Title	Date
552.215-70	EXAMINATION OF RECORDS BY GSA	FEB 1996
552.232.25	Prompt Payment	(Nov 2009)

I.11 GSAM 552.203-71 RESTRICTION ON ADVERTISING (SEP 1999)

The Contractor shall not refer to this contract in commercial advertising or similar promotions in such a manner as to state or imply that the product or service provided is endorsed or preferred by the White House, the Executive Office of the President, or any other element of the Federal Government, or is considered by these entities to be superior to other products or services. Any advertisement by the Contractor, including price-off coupons, that refers to a military resale activity shall contain the following statement: "This advertisement is neither paid for nor sponsored, in whole or in part, by any element of the United States Government."

I.12 GSAM 552.232-72 FINAL PAYMENT (SEP 1999)

Before final payment is made, the Contractor shall furnish the Contracting Officer with a release of all claims against the Government relating to this contract, other than claims in stated amounts that are specifically excepted by the Contractor from the release. If the Contractor's claim to amounts payable under the contract has been assigned under the Assignment of Claims Act of 1940, as amended (31 U.S.C. 3727, 41 U.S.C. 15), a release may also be required of the assignee.

I.13 GSAM 552.252-6 AUTHORIZED DEVIATIONS IN CLAUSES (SEP 1999)

(a) *Deviations to FAR clauses*.

(1) This solicitation or contract indicates any authorized deviation to a Federal Acquisition Regulation (48 CFR Chapter 1) clause by the addition of "(DEVIATION)" after the date of the clause, if the clause is not published in the General Services Administration Acquisition Regulation (48 CFR Chapter 5).

(2) This solicitation indicates any authorized deviation to a Federal Acquisition Regulation (FAR) clause that is published in the General Services Administration Acquisition Regulation by the addition of "(DEVIATION (FAR clause no.))" after the date of the clause.

(b) *Deviations to GSAR clauses*. This solicitation indicates any authorized deviation to a General Services Administration Acquisition Regulation clause by the addition of "(DEVIATION)" after the date of the clause.

(c) *"Substantially the same as" clauses*. Changes in wording of clauses prescribed for use on a "substantially the same as" basis are not considered deviations.

I.14 DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENTS (DFARS) CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

Defense Procurement website: www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

Clause No	Clause Title	Date
252.204-7000	Buy American Act – Balance of Payments Program Certificate	(Dec 2009)
252.204-7001	Buy American Act AND Balance of Payments Program	(Oct 2011)
252.204-7004	Alternate A, Central Contract Registration	(Sep 2007)
252.216-7005	Award Fee	(Feb 2011)
252.216-7999	Award Fee Reduction or Denial for Jeopardizing the Health or Safety of Government Personn	(Apr 2010)
252.225-7012	Preference for Certain Domestic Commodities	(June 2010)
252.225-7040	Contractor Personnel Authorized to Accompany U.S. Armed Forces Deployed Outside the United States	(June 2011)
252.225-7043	Antiterrorism/Force Protection for Defense Contractors Outside the United States	(March 2006)
252.227-7013	Rights in Technical Data – Noncommercial Items	(Mar 2011)
252.227-7014	Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation	(Mar 2011)
252.227-7015	Technical data—Commercial items	(Nov 1995)
252.227-7016	Rights in Bid or Proposal Information	(Jan 2011)
252.227-7017	Identification and assertion of use, release, or disclosure restrictions.	(Jun 1995)
252.227-7019	Validation of Asserted Restrictions – Computer Software	(Jun 1995)
252.227-7023	Drawings and Other Data to Become Property of Government	(Mar 1979)

Clause No	Clause Title	Date
252.227-7025	Limitations on the Use or Disclosure of Government-Furnished Information Marked With Restrictive Legends	(Jun 1995)
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government	(Jun 1995)
252.227-7030	Technical Data—Withholding of Payment	(Mar 2000)
252.227-7037	Validation of Restrictive Markings on Technical Data	(Sep 1999)
252.228-7000	Reimbursement for War Hazard Losses	(Dec 1991)
252.228-7003	Capture and Retention	(Dec 1991)
252.243-7002	Requests for Equitable Adjustment	(Mar 1998)
252.246-7001	Warranty of Data	(Dec 1991)

I.15 AFFAR CLAUSES INCORPORATED BY REFERENCE

The full text of a provision may be accessed electronically at:

http://farsite.hill.af.mil/vfafara.htm

Clause No	Clause Title	Date
5352.201-9101	Ombudsman	(Apr 2010)
5352.242-9001	Contractor Access to Air Force Installations	(June 2007)

I.15.1 Ombudsman
ACQUISITION POLICY, INTEGRITY, AND WORKFORCE (MVA)

The Office of General Services Acquisition Policy, Integrity, & Workforce promotes and monitors GSA's activities supporting acquisition integrity--a fair and balanced approach for conducting acquisitions in an ethical manner in accordance with federal acquisition procedures. The Suspension & Debarment, & Contract Remedies (SDCR) Division reviews reports on contractors, generally from the Office of the Inspector General, to determine if they are presently responsible to contract with the federal government. The Procurement Management Review Division (PMR), mainly through on site visits to GSA contracting activities, assesses and reports on compliance with statutory, regulatory, and policy guidance, as well as sound business practices. The General Services Acquisition Policy Division (GSAP) establishes and implements acquisition policies for the agency fulfilling immediate and long term acquisition goals and priorities. The General Services Acquisition Workforce Division (GSAW) works to ensure the agency's acquisition workforce maintains a high caliber of acquisition capabilities, and certifies their ability to fulfill the agency's acquisition needs. Other functions of the Office include: Agency Protest Official; Task and Delivery Order Ombudsman; Agency Competition Advocate; and, Construction Metrication

The POC listed is Virginia Huth: (202) 208-5028

The information provided in Section J is for reference only. The documents in Section J are not intended to change the TOR and any conflict therein should be resolved by referring and relying upon the TOR. Because the Section J reference materials may be outdated or contain information that has not been recently verified for accuracy, the Government does not warrant the accuracy of the information for purposes of this TOR.

J.1 LIST OF ATTACHMENTS

Attachment A	COR Appointment Letter
Attachment B	Award Fee Determination Plan
Attachment C	Attachment Deleted
Attachment D	DD 254 (separately attached)
Attachment E	Employee/Contractor Non-Disclosure Agreement
Attachment F	Travel Authorization
Attachment G	Attachment Deleted
Attachment H	Attachment Deleted
Attachment I	Quality Assurance Surveillance Plan (QASP)
Attachment J	Acronym List
Attachment K	Problem Notification Report
Attachment L	Attachment Deleted
Attachment M	Consent to Purchase form
Attachment N	Regulations and Publications
Attachment O	Deliverable Acceptance-Rejection Report
Attachment P	Background and Sizing Information
Attachment Q	Monthly Status Report
Attachment R	Non-Key Personnel Knowledge and Skills
Attachment S	Incremental Funding Table

Attachment A
COR Appointment Letter

Attachment B

Award Fee Determination Plan

AWARD FEE DETERMINATION PLAN

FOR

UNITED STATES CENTRAL COMMAND

SECTION 1: INTRODUCTION

This Award Fee Determination Plan (AFDP) provides procedures for evaluating the Contractor's performance on the USCENTCOM Task Order (TO) on a Cost-Plus-Award-Fee (CPAF) basis in accordance with (IAW) Section H.26.2 of the Federal System Integration and Management (FEDSIM), Federal Acquisition Service (FAS) Task Order Request (TO) #GST0012AJ0127. The AFDP is applicable only to CPAF CLINs X001 through X002. The award fee objective for this TO is to afford the Industry Partner the opportunity to earn award fee commensurate with optimum performance:

- By providing a workable award fee plan with a high probability of successful implementation;
- By clearly communicating evaluation procedures that provide effective two-way communication between the Industry Partner and the Government; and
- By focusing the Industry Partner on areas of greatest importance in order to motivate outstanding performance.

The amount of the Award Fee earned and payable to the Contractor for achieving specified levels of performance will be determined by the Award Fee Determination Official (AFDO), with the assistance of the Award Fee Evaluation Board (AFEB), per this plan. The maximum fee payable is 100% of the Award Fee. The Contractor may earn all, or part, or none of the Award Fee allocated to an evaluation period.

If a contract with an award-fee clause is terminated for convenience of the Government after the start of an award-fee evaluation period, the earned award-fee amount should be determined by the FDO using the normal award-fee evaluation process. The remaining available award-fee dollars for all subsequent evaluation periods should not be considered available or earned and, therefore, should not be paid.

This AFDP may be amended IAW Section H.26.2 of this TO.

SECTION 2: EVALUATION PERIODS

2.1 The first and second award fee periods will consist of ninety day increments. Thereafter, the Government will evaluate Contractor performance every six months for determining award fee payment. The initial year award fee period will cover the 6-month period at the beginning of the period of performance (September 7, 2012 – March 6, 2013). The second award fee period will cover March 7 – September 6, 2013. For the remainder of the task order, the Government will evaluate Contractor performance every six months for determining award fee payment. Mid-Period reviews will be scheduled concurrent with in-process reviews as practicable.

2.2 The Government will determine the award fee payment by the last workday of the month following the performance period. The following table shows the expected performance periods and the dates of award fee determination.

Award Fee					
Year	**Period**	**Months Covered**	**Available Award Fee Pool**	**Earned Fee**	**Unearned Fee**
Base Year	1	Sep 7, 2012 – Mar 6, 2013	(b) (4)	(b) (4)	(b) (4)
Base Year	2	Mar 7 - Sep 6, 2013	(b) (4)	(b) (4)	(b) (4)
Option Year 1	3	Sep 7, 2013 – Mar 6, 2014	(b) (4)	(b) (4)	(b) (4)
Option Year 1	4	Mar 7 - Sep 6, 2014	(b) (4)	(b) (4)	(b) (4)
Option Year 2	5	Sep 7, 2014 – Mar 6, 2015	(b) (4)	(b) (4)	(b) (4)
Option Year 2	6	Mar 7 - Sep 6, 2015	(b) (4)		
Option Year 3	7	Sep 7, 2015 – Mar 6, 2016	**TBD**		
Option Year 3	8	Mar 7 - Sep 6, 2016	**TBD**		
Option Year 4	9	Sep 7, 2016 – Mar 6, 2017	**TBD**		
Option Year 4	10	Mar 7 - Sep 6, 2017	**TBD**		

These time frames can be changed at the unilateral discretion of the Government.

SECTION 3: AWARD FEE ALLOCATION FORMULA

3.1 The maximum award fee pool will be determined for each year of estimated labor costs as awarded in this TO. The yearly pool will be comprised of an award fee amount identified in Section B of this TO. This total comprises the maximum award fee pool for the year being calculated. This pool will then be divided in half to provide for the six month performance periods. The maximum available award fee for a given six month performance period is then one half of the annual pool. The Government will adjust the award fee pool to be proportional to the level of effort/cost incurred during the award fee evaluation period.

3.2 The following table shows the allocation percentage by scores. The definition for each rating adjective is shown in Section 3.3. (The percentages in this section are prescribed in FAR 16.401(e)(3)(iv).)

Rating	**Percentage of Fee**
Excellent	91%-100%
Very Good	76%-90%
Good	51%-75%
Satisfactory	No Greater than 50%
Unsatisfactory	0%

3.3 SATISFACTION GRADE SCALE (BY CATEGORY) The performance categories, once graded, describes the overall customer satisfaction with the task key indicators. Contained in the ratings is a word picture of standards that allows each monitor to work from a common grading scale. (The adjectival ratings and descriptions in this section are prescribed in FAR 16.401(e)(3)(iv). Per that section of the FAR, the Contracting Officer may choose to supplement the adjectival rating descriptions included in this section.)

EXCELLENT

Contractor has exceeded almost all of the significant award-fee criteria and has met overall cost, schedule, and technical performance requirements of the contract in the aggregate as defined and measured against the criteria in the award-fee plan for the award-fee evaluation period.

VERY GOOD

Contractor has exceeded many of the significant award-fee criteria and has met overall cost, schedule, and technical performance requirements of the contract in the aggregate as defined and measured against the criteria in the award-fee plan for the award-fee evaluation period.

GOOD

Contractor has exceeded some of the significant award-fee criteria and has met overall cost, schedule, and technical performance requirements of the contract in the aggregate as defined and measured against the criteria in the award-fee plan for the award-fee evaluation period

SATISFACTORY

Contractor has met overall, cost, schedule, and technical performance requirements of the contract in the aggregate as defined and measured against the criteria in the award fee plan for the award fee evaluation period.

UNSATISFACTORY

Contractor has failed to meet overall cost, schedule, and technical performance requirements of the contract in the aggregate as defined and measured against the criteria in the award-fee plan for the award-fee evaluation period.

SECTION 4: ORGANIZATIONAL STRUCTURE OF AWARD FEE DETERMINATION

4.1 Award Fee Determination Official and Client Award Fee Recommending Official

The Chair of the AFEB is responsible for gathering Contractor observation reports (scorecards) from the performance monitors for each evaluation period and preparing the award fee board recommendation. The COR will gather the last month's scorecards and consolidate the scorecards covering the six month award fee period (AFP) and present the baseline evaluation information to the AFEB. The Chair of the AFEB shall invite the Contractor to present a self-assessment of their performance for the period. The Contractor has one hour to present the self assessment before the AFEB deliberates over the final award fee recommendation. The AFEB must have 75% of its voting members present to make an official recommendation. Both the AFEB report and Contractor's self-assessment will be provided to the Client Award Fee Recommending Official (CAFRO) for consideration.

The CAFRO will consider the final AFEB report and discuss it if necessary with the board. The CAFRO may accept, reject, or modify the AFEB recommendation. The CARFO's recommendation of the award fee amount of award fee earned and the basis of the recommendation will be stated in an Award Fee recommendation report and forwarded to the AFDO. The AFDO will consider the CAFRO recommendation and discuss it if necessary with the CAFRO and the board. The AFDO may accept, reject, or modify the CAFRO recommendation. The AFDO and the CO will make the final determination of the award fee earned during the period. The AFDO's determination of the award fee amount of award fee earned and the basis of the determination will be stated in an Award Fee determination report and forwarded to the CO.

The CO will be responsible for monitoring and evaluating administrative aspects of the Contractor's performance. The CO will also be responsible for reviewing and assessing the documentation produced by the COR.

The determination of the AFDO (including the amount of the award fee), the determination of Contractor performance against the award fee criteria, and the assessment of the nature and success of the Contractor's performance is final and not subject to the Disputes clause of the basic contract.

The Government may unilaterally change the award fee plan and evaluation criteria at any time before the applicable award fee period in an effort to continuously fine-tune the criteria and areas of emphasis as lessons are learned and better performance metrics are identified.

4.1.1 Award Fee Determination Official (AFDO)

The AFDO is the Group Manager (GM), FEDSIM. The Contracting Officer (CO) will appoint the AFDO in writing.

The AFDO's responsibilities are:

- Approve the Award Fee Plan and authorize any changes to the Award Fee Plan throughout the life of the TO.
- Approve the members of the Award Fee Evaluation Board (AFEB) and appoint the AFEB Chairperson.
- Review assessments of Contractor performance. This will include ensuring that the documentation contains sufficient information substantiating the fairness and reasonableness of the award fee decision. Feedback coordinated with the AFEB will be provided to the Contractor as appropriate during the evaluation period to enhance overall performance and minimize problems.
- Determine the amount of award fee the Contractor has earned based on its performance during each evaluation period.

4.1.2 Client Award Fee Recommending Official (CAFRO)

The CAFRO is the Client Agency's Director (CCJ6) or Deputy Director. The CAFRO reviews the AFB Report and recommends the earned award fee amount for each evaluation period to the AFDO.

4.2 Award Fee Evaluation Board (AFEB)

The AFEB has a chairperson, the Client Resources Division Chief (CCJ6-R). Other voting members of the board are the FEDSIM Contracting Officer's Representative (COR) and Government representatives from the Client Organization. The FEDSIM CO is a non-voting advisory member of the AFEB. Additional non-voting board members may be USCENTCOM Government or military performance monitors as deemed appropriate by the AFEB chairman. The following table provides the individuals that are members of the AFEB. Substitutions are permitted in the event of a schedule conflict, subject to approval by the AFEB Chairperson. Attendance of the non-voting members is not required to convene a board.

Board Position	Title
Chairperson	Client Resources Division Chief (CCJ6-R)
AFEB Voting Member	Client Agency Technical Point of Contact
AFEB Voting Member	CCJ6 division QAE
AFEB Voting Member **	CCJ6 division QAE
AFEB Voting Member **	CCJ6 division QAE
AFEB Voting Member **	CCJ6 division QAE

AFEB Voting Member **	CCJ6 division QAE
AFEB Voting Member **	CCJ6 division QAE
AFEB Voting Member	FEDSIM COR
AFEB Non-Voting Member	FEDSIM CO
AFEB Non-Voting Member(s)	CLIENT NAME
AFEB Non-Voting Member	Secretary

** Optional seats. AFEB Chairperson may appoint as many AFEB Voting members as desired but must have three voting members in addition to the Chairperson**.**

Non-voting members will participate in AFEB assessments of Performance Monitor (PM) evaluations and discussions of award fee recommendations. Additionally, non-voting members are allowed to submit written reports on Contractor performance to the AFEB, for its consideration.

The responsibilities of the AFEB are:

a. Recommend to the CAFRO and AFDO the specific elements upon which the Contractor will be evaluated for each evaluation period.

b. Request and obtain performance information from performance monitors involved in observing Contractor performance.

c. Evaluate the Contractor's performance and summarize its findings and recommendations for the CAFRO and AFDO.

d. Recommend to the CAFRO and AFDO the percentage of award fee available during an evaluation period which the Contractor should receive.

4.2.1 AFEB Chairperson

The responsibilities of the AFEB Chairperson are to:

a. Appoint an AFEB Secretary.

b. Conduct AFEB meetings.

c. Resolve any inconsistencies in the AFEB evaluations.

d. Ensure AFEB recommendations to the AFDO are timely and made in accordance with the Award Fee Agreement and this plan.

e. Ensure timely payment of award fee earned by the Contractor.

f. Recommend any changes to the Award Fee Plan to the AFDO.

g. Ensure and have overall responsibility for the proper execution of the AFDP including managing the activities of the AFEB.

h. Exerts overall responsibility for all documents and activities associated with the AFEB.

4.2.2 AFEB Secretary

The responsibilities of the AFEB Secretary are to:

a. Review PM reports and other performance information and present an overview to the AFEB, as well as all supporting data.

b. Consolidate the AFEB's assessment and recommendation for presentation to the CAFRO and AFDO at both the midterm and final stages of each evaluation period.

c. Draft all correspondence required by the CAFRO, AFDO, and AFEB as it relates to the award fee process.

d. Maintain the Award Fee Plan, including any updates as approved by the AFEB and the AFDO, and modified in the TO.

e. Select a separate AFEB recorder, if desired, who will maintain the AFEB minutes, notify AFEB board members and performance monitors of report due dates and meeting times, distribute forms, and receive and distribute completed reports to all members.

f. Maintain the award fee files, including current copies of the Award Fee Plan, any internal procedures, performance monitor's reports, and any other documentation having a bearing on the AFDO's award fee decisions.

4.2.3 Quality Assurance Evaluators (QAE)/Performance Monitors (PMs)

Government and TO support personnel will be identified by the AFEB Chairperson as QAEs/performance monitors to aid the AFEB in making its recommendation for award fee. Quality Assurance Evaluators (representing each division) and PMs (responsible for the technical administration of specific tasks issued under the contract) document the Contractor's performance against evaluation criteria in their assigned evaluation areas(s). QAEs' and PMs' primary responsibilities include (1) monitoring, evaluating, and assessing Contractor performance in assigned areas, (2) preparing evaluation reports (scorecards) that ensure a fair and accurate portrayal of the Contractor's performance, and (3) recommending changes to the plan. These QAEs and PMs will submit written reports, as required by the AFEB Chairperson, on the Contractor's performance to the AFEB for consideration. Submission of their reports will be coordinated through the AFEB Secretary. Procedures and instructions for the performance monitors regarding mid-term and final evaluations are provided below. The final report will be comprehensive and will be completed and submitted to the AFEB Secretary in accordance with the schedule below, unless otherwise notified in writing of any changes.

5.0 AWARD FEE DETERMINATION PROCESS

The Contractor begins each evaluation period with 0 % of the available award fee and works up to the earned award fee based on performance during the evaluation period.

5.1 Monitoring and Assessing Performance

The AFEB chairperson will assign QAEs/PMs for the major performance areas. The PMs will be selected on the basis of their expertise in the prescribed performance areas and/or their association with specific technical tasks. The AFEB chairperson may assign and change QAEs/PMs assignments at any time and will notify the Contractor. The AFEB chairperson will ensure that each monitor and board member has copies of the TO and all modifications, a copy of this plan, and all changes and specific instructions for assigned areas.

QAEs/PMs will conduct assessments of the Contractor performance in their assigned areas. Feedback coordinated with the AFEB Chairperson will be provided to the Contractor as appropriate during the evaluation period to enhance overall performance and minimize problems.

5.1.1 Instructions for QAEs/PMs

QAEs/PMs will maintain a periodic written record of the Contractor's performance, including inputs from other Government personnel, in the evaluation areas of responsibility. QAEs/PMs will retain informal records used to prepare evaluation reports for twelve months after the completion of an evaluation period to support any inquires made by the AFDO. QAEs/PMs will conduct assessments in an open, objective, and cooperative spirit, so that a fair and accurate evaluation is made. PMs will make every effort to be consistent from period to period in their approach to determine recommended ratings. Positive accomplishments should be emphasized just as readily as negative ones.

a. Performance Monitor Evaluation Reports. QAEs/PMs will prepare midterm and final evaluation reports for each evaluation period during which they are performance monitors. The final reports will be more comprehensive. The reports, as a minimum, contain the following information:

    1) The criteria and methods used to evaluate the Contractor's performance during the evaluation period.

    2) The technical, economic and schedule environment under which the Contractor was required to perform. What effect did the environment have on the Contractor's performance?

    3) The Contractor's major strengths and weaknesses during the evaluation period. Give examples of the Contractor performance for each strength and weakness listed. Also provide the reference in the specification, statement of work, data requirement, task order etc. that relates to each strength or weakness.

4) A recommended rating for the evaluation period using the adjectives and their definitions set forth in this award fee plan. Provide concrete examples of the Contractor's performance to support the recommended rating.

5.2 Procedures for Award Fee Evaluations

These procedures provide for both a midterm evaluation and full-rating-period evaluation. Procedures common to both evaluations are listed first, followed by the procedures unique to each evaluation.

5.2.1 Common Procedures

5.2.1.1 Exclusions

Throughout the entire evaluation period, the Contractor shall present and document any exclusion to the period of performance, due to circumstances beyond the control of the Contractor, to the AFEB Chairperson in accordance with the Award Fee Process Timeline in Section 5.2.4.9. The performance monitors should present the exclusions (if any) to the AFEB. If necessary, the AFEB will ask the Contractor to present their case. The AFEB in conjunction with the FEDSIM CO will make a unilateral decision as to the exclusion from the evaluation.

5.2.1.2 Contractor Monthly Performance Reports

The Contractor shall prepare Monthly Performance Reports including the Section F Deliverable that contains data that can be used to compare against the Performance Standards stated in this Award Fee Plan. All Performance Reports, including the raw data, shall be provided to the designated performance monitors in accordance with the Award Fee Process Timeline in Section 5.2.4.9.

5.2.2 Monthly Report Review

PMs will collect the Monthly Performance Reports from the Contractor which they will review and analyze for accuracy and if required provide an oral or written summary to the AFEB. If required, these summaries shall be provided in accordance with the Award Fee Process Timeline in Section 5.2.4.9.

5.2.3 Midterm Evaluation Procedures

The purpose of the midterm evaluation is to provide the Contractor a quick, concise, interim Government review of the Contractor performance, and provide the Contractor an opportunity to improve its performance prior to the determination of award fee earned at the end of the evaluation period. No award fee is paid based on midterm evaluations.

5.2.3.1 Midterm Evaluation Reports

The performance monitors will provide midterm evaluations for each evaluation period. Midterm reports will be submitted to the AFEB Secretary in accordance with the Award Fee Process Timeline in Section 5.2.4.9.

5.2.3.2 AFEB Midterm Evaluation and Report

The AFEB, after receipt of the Contractor's self evaluation, will meet and evaluate all performance information it has obtained. The AFEB will review the performance monitors' reports and prepare a midterm evaluation report. The report will be developed using the format contained in Appendix 2.

5.2.3.3 Contractor Notification Letter

The AFEB Secretary will prepare a resultant summary report for AFEB Chairperson approval. The AFEB Chairperson will use this letter to inform the Contractor orally of the Government's midterm evaluation in accordance with the Award Fee Process Timeline in Section 5.2.4.9.

5.2.4 Award Fee Evaluation Procedure

This procedure is designed to ensure that Award Fee Evaluation takes place in a timely and effective manner with proper documentation. The Award Fee Board should meet after the end of evaluation period in accordance with the Award Fee Process Timeline in Section 5.2.4.9. The AFEB must have 75% of voting members present to make an official recommendation. The AFEB will document the performance to substantiate the assigned score or ratings as appropriate.

5.2.4.1 Contractor Self Evaluation

After the rating period has ended the Contractor shall provide its self-evaluation to the AFEB chairperson in accordance with the Award Fee Process Timeline in Section 5.2.4.9. This self-assessment should be written with the option of presenting an oral self-assessment if requested by the board.

5.2.4.2 Performance Monitor Final Reports

The PMs will provide evaluations for the entire six-month evaluation period. PMs will submit final evaluation reports after the end date of the evaluation period to the AFEB Secretary in accordance with the Award Fee Process Timeline in Section 5.2.4.9. The final reports will be more comprehensive than the midterm reports.

5.2.4.3 Contractor Self Evaluation Presentation

The AFEB may request a presentation of the findings of the Contractor's self evaluation prior to the AFEB Meeting to discuss the report's preliminary finding and recommendations. This presentation generally lasts no longer than one hour. If necessary, a subsequent question-and-answer session is permissible.

5.2.4.4 AFEB Meeting and Memorandum to the AFDO

The AFEB, after receipt of the Contractor's self evaluation, will meet and evaluate all performance information it has obtained. The AFEB will review the PMs' reports and prepare an Award Fee evaluation report. The report will be a memorandum to the AFDO with the AFEB's recommendation. The report will recommend the award fee amount and any unresolved the Contractor issues to the AFDO. The report will be developed using the format contained in Appendix 2.

5.2.4.5 CAFRO Final Report

After meeting with the AFEB Chairman, the CAFRO and AFEB will finalize the report and present it to the AFDO in accordance with the Award Fee Process Timeline in Section 5.2.4.9

5.2.4.6 Award Fee Determination Report

The AFDO will consider the final AFEB report and ensure compliance with the Award Fee Determination Plan. The AFDO may accept, reject, or modify the AFEB recommendation. The AFDO will make the final determination of the award fee earned during the period. The AFDO's determination of the award fee amount of award fee earned and the basis of the determination will be stated in an Award Fee determination report and forwarded to the FEDSIM CO for the TO file. The report will be developed using the format contained in Appendix 1.

5.2.4.7 Award Fee Determination Notice

The FEDSIM CO will prepare this notice to the Contractor stating the amount of the award fee earned for the evaluation period.

5.2.4.8 Contractor Invoice

The Contractor shall invoice without a modification after receipt of the award fee determination notice.

5.2.4.9 Award Fee Process Timeline

Procedures Paragraph Reference	Procedure	Responsible Party	Due Date
Common Procedures to both Mid-Term and Final Evaluation Periods			
7.1.1	Exclusions	Contractor	As required, within 5 workdays of occurrence
7.1.2	Monthly Performance Report	Contractor	Incorporated in the Contractor's Monthly Status Report
7.1.3	Contractor's Monthly Status Report	Contractor	10th calendar day of each month
7.1.4	Monthly Report Review	Government	5 workdays after receipt of Contractor's Monthly Status Report, if needed
Mid-Term Evaluation Procedures			

Procedures Paragraph Reference	Procedure	Responsible Party	Due Date
7.2.2.2	Evaluator Monthly Evaluation Reports	Government	15 workdays after the end of the Month
7.2.2.2	Evaluator Midterm Evaluation Reports	Government	15 workdays after the end of the Midterm Period
7.2.2.1	Contractor Self-Evaluation	Contractor	15 workdays after the end of the Midterm Period
7.2.2.3	AFEB Midterm Evaluation and Summary Evaluation Report	Government	20 workdays after the end of the Midterm Period
7.2.2.4	Contractor Notification	Government	25 workdays after the end of the Midterm Period
7.2.2.5	Contractor Mitigation Letter, and/or Contractor Conference If requested by either the Contractor or the AFEB.	Contractor	30 workdays after the end of the Midterm Period
Final Evaluation Procedures			
7.3.2	Evaluators' Final Reports	Government	15 workdays after the end of the Full Period
7. 3.1	Contractor Self-Evaluation	Contractor	15 workdays after the end of the Full Period
7.3.3	AFEB Meeting and Summary Evaluation Report	Government	20 workdays after the end of the Full Period
7.3.4	Award Fee Determination Memorandum	Government	25 workdays after the end of the Full Period
7.3.5	Contractor Notification	Government	30 workdays after the end of the Full Period
7. 3.6	Contractor Invoice	Contractor	Determined by the Contractor

Procedures Paragraph Reference	Procedure	Responsible Party	Due Date
7.3.7	Contractor Mitigation Letter, and/or Contractor Conference If requested by either the Contractor or the AFEB	Contractor	35 workdays after the end of the Full Period, if desired or requested

SECTION 6: EVALUATION CRITERIA AND WEIGHTS

The AFDP consists of award fee provisions for four distinct areas. The award fee areas are broken down as follows:

20% Measurement Area 1 Task Order Management

10% Measurement Area 2 Personnel Management

10% Measurement Area 3 Financial Management

60% Measurement Area 4 Technical Effectiveness

100% Total

The criteria and weights provided below are guidelines to be used in evaluating these areas to determine the appropriate award fee. Members of the AFEB and working group will use the following examples of criteria and sub-criteria to evaluate the Contractor's performance during each award fee evaluation period.

The questions identified in this section with an emphasis on Transition, will be used in the determination of the Contractor's award fee in the first award fee determination cycle. Current performance metrics/subjective elements will be used to determine the Contractor's award fee in the first award fee period.

Performance metrics and other subjective criteria may be revised for subsequent award fee periods. Those future performance metrics will be developed jointly by the Contractor and Government and may replace some or all of the criteria listed below. The Government has the final say as to what performance metrics will be incorporated.

The rating scale and criteria on the following pages will be used in the evaluation. The percentage of the Award Fee which corresponds to these ratings also is indicated. All sub criteria possess an equivalent weight within the parent criteria.

- **Measurement Area 1 – Task Order Management 20 %**
  - Schedules and Timeliness
  - Responsive to Customer Needs (internal as well as external customers)
  - Documentation – (i.e., reports, plans, operational procedures)
  - Project Management – The Contractor is expected to measure the effectiveness and efficiency of project management activities from small team projects to larger projects that may require cross-divisional coordination. Measurement includes developing and executing plans for requirements management; project management, oversight, and tracking; cross section and cross division projects, quality assurance, configuration management, logistics support, and out-year support.
  - Process Improvement – The Contractor is expected to continuously improve business processes through effective defect prevention programs, and change management plans for technology and processes. Measurement includes reviews and proposals to improve work centers.
  - Continuity of Operations – the Contractor is expected to contribute to the overall contingency plan and then execute as required. The Contractor must identify emergency action plan personnel based on scenarios provided by CCJ6 or identified by the Contractor required to execute contingency operations.
  - Develop and update the Task Order Management Plan (TOMP) and map to the J6 vision (500 Day Plan) and mission changes.
  - Quality and Productivity Assessment – the Contractor is expected to provide and document a consistent approach for capturing quality and productivity measurement data and compare actual results with forecasts for both products and processes. Perform root cause analysis to mitigate recurring problems and recommend solutions.
  - Proactive communication
    - Identify opportunities to improve the J6 IT environment and to gain efficiencies
    - Provides alternatives to allow government to meet surge requirements or changes, within budget and minimizing impact to current operations
    - Quickly identify issues and seek resolution

- **Measurement Area 2 – Personnel Management 10 %**
    - Turnover - Continuity of operations is damaged by excessive turnover. Proactive management of turnover to minimize operational impact. Provide trend analysis on turnover to identify possible trouble spots and provide resolutions to trouble areas.
    - Training and Staff Development – The Contractor is expected to invest in appropriate training for the staff assigned to this project as a commitment to excellence.
    - Coverage/Deployment - Measured by how well the vendor is able to plan and adjust for staffing changes that are demanded by the operational tempo and the dynamic environment USCENTCOM anticipates.
    - Maximize personnel resource planning to gain efficiencies and to reduce cost. Right size the workforce to meet task needs.
    - Training and Staff Development – A measure of how well contract employees are current with the latest industry advancements. Contract staff is expected to maintain industry standard certification levels and attend Contractor-funded training, as well as seminars and trade shows to maintain proficiency.

- **Measurement Area 3 – Financial Management 10 %**
    - Cost Containment and Efficiencies - The Contractor will be graded on cost estimates and efficient use of contractor and Government resources. The management of cost for ongoing services, and presentation of cost mitigation strategies. Financial Reporting – contract costs and hours expended against annual work plan tasks (by CLINs) timely accurate reports of expenditures against baseline with trend analysis to anticipate possible cost overruns or to discover efficiencies. Track and report (by CLINs), what hours and funds are still available by period (by CLINs), and forecast when the funding has expended (by CLINs).
    - Provide cost Forecasting – for legacy systems and estimate operational cost for future systems and or new configurations to ensure accurate operational costs are projected and the future impact of projects requiring services maintenance are included in the revised baseline for government program managers.
    - Accuracy and clarity of invoices- Invoicing is viewed as management tool and will be used to anticipate future costs as well as evaluating past progress. The program managers and TPOC must be able to identify costs in varying degrees of detail depending on circumstances and DoD guidance.

- **Measurement Area 4 - Technical Effectiveness 60 %**
    - Implementation and integration of new hardware, software, procedures, and tech refresh procedures to assist in process improvement, system reliability, system

capability, and operational efficiency – measurement includes developing suitable training programs and logistics support plans for newly accepted technologies.

- Technology Insertion and Exploitation - A measure of how well the vendor does in providing new solutions as well as working to get the most out the legacy systems already in service. The Contractor must explore and propose new solutions and/or upgrades to meet missions. The Contractor must review current levels of services and then propose and demonstrate enhancements. Prospective solutions must be evaluated against command requirements.
- Routine Operation and Maintenance – A measure of how well the Contractor completes all work. The measurement will consist of how well the Contractor meets the agreed upon performance metrics in their Quality Control Plan.

APPENDIX 1: AFEB Summary Evaluation Report

Date:

AFEB Chairperson Name:
Award Fee Period: from _____ to _____
(Attach additional pages, supporting data, etc. as needed.)

Criteria 1 – Task Order Management: Rating Adjective/Performance Points

Discussion:

Strengths:

Weaknesses:

Criteria 2 – Personnel Management: Rating Adjective/Performance Points

Discussion:

Strengths:

Weaknesses:

Criteria 3 – Financial Management: Rating Adjective/Performance Points

Discussion:

Strengths:

Weaknesses:

Criteria 4 – Technical Effectiveness: Rating Adjective/Performance Points

Discussion:

Strengths:

Weaknesses:

Award fee rating recommended for this evaluation criteria and period of performance with recommended percentage earned.

AFB Chairperson Signature: _____

APPENDIX 2: AFEB Evaluator's Report

Instructions: Evaluators are requested to use bulletized format for submitting strengths, weaknesses and recommendations. Also, evaluators are encouraged to attach additional sheets, supporting data, etc. for the final report.

Date:
Evaluator Name and Title:
Award Fee Period: from _____ to _____
Evaluator's Primary Task Area(s) (check all that apply):

	Criteria 1 – Task Order Management
	Criteria 2 – Personnel Management
	Criteria 3 – Financial Management
	Criteria 4 – Technical Effectiveness

Note: Evaluators are NOT limited to evaluating only their own task areas. Experiences in other areas should also be evaluated. However, please indicate in the boxes above your primary area(s) of responsibility.

Special Circumstances during this period and their impact:

Strengths of the Contractor's performance:

Weaknesses in the Contractor's performance (with examples and contract references):

Impact of the Contractor's performance on execution of the program:

Corrective actions recommended, if any:

Award fee rating recommended for this evaluation criteria and period of performance (with supporting examples):

Evaluator Signature: _____

Attachment C
Attachment Deleted

Attachment D
DD 254
(Separtely attached)

\\

Attachment E
NON-DISCLOSURE AGREEMENT
BETWEEN
U.S. GENERAL SERVICES ADMINISTRATION (GSA)
FEDERAL SYSTEMS INTEGRATION AND MANAGEMENT CENTER (FEDSIM)
AND
[CONTRACTOR]

This agreement, made and entered into this _____ day of _____, 20XX (the "Effective Date"), is by and between GSA and [CONTRACTOR].

WHEREAS, [CONTRACTOR] and GSA FEDSIM have entered into [Contract No.], Task Order No. [INSERT] for services supporting USCENTCOM;

WHEREAS, [CONTRACTOR] is providing C4 Enterprise Support services under the Task Order;

WHEREAS, the services required to support USCENTCOM involve certain information which the Government considers to be "Confidential Information"[1] as defined herein;

WHEREAS, GSA desires to have [CONTRACTOR]'s support to accomplish the Task Order services and, therefore, must grant access to the Confidential Information;

WHEREAS, [CONTRACTOR] through its work at a Government site may have access to Government systems or encounter information unrelated to performance of the Task Order which also is considered to be Confidential Information as defined herein;

WHEREAS, GS on behalf of USCENTCOM desires to protect the confidentiality and use of such Confidential Information;

NOW, THEREFORE, for and in consideration of the mutual promises contained herein, the parties agree as follows:

1. **Definitions.** "Confidential Information" shall mean any of the following: (1) "contractor bid or proposal information" and "source selection information" as those terms are defined in 41 U.S.C. § 2101; (2) the trade secrets or proprietary information of other companies; (3) other information, whether owned or developed by the Government, that has not been previously made available to the public, such as the requirements, funding or budgeting data of the Government; and *for contracts/orders providing acquisition assistance*, this term specifically includes (4) past performance information, actual/proposed costs, overhead rates, profit, award fee determinations, contractor employee data of offerors/contractors, methods or procedures used to evaluate performance, assessments, ratings or deliberations developed in an evaluation process, the substance of any discussions or deliberations in an evaluation process, and any recommendations or decisions of the Government unless and until such decisions are publicly announced. This term is limited to unclassified information.

2. **Limitations on Disclosure.** [CONTRACTOR] agrees (and the [CONTRACTOR] Task Order personnel must agree by separate written agreement with CONTRACTOR) not to distribute, disclose or disseminate Confidential Information to anyone beyond the personnel identified in the [ATTACHED ADDENDUM], unless authorized in advance by the GSA Contracting Officer in writing. The Contracting Officer and [CLIENT POC] will review the Addendum to ensure it includes only those individuals to be allowed access to the information. The Addendum, which may be updated from time to time, is approved when signed by the GSA Contracting Officer and [CLIENT POC].

[1] This does not denote an official security classification.

3. **Agreements with Employees and Subcontractors.** [CONTRACTOR] will require its employees and any subcontractors or subcontractor employees performing services for this Task Order to sign non-disclosure agreements obligating each employee/subcontractor employee to comply with the terms of this agreement. [CONTRACTOR] shall maintain copies of each agreement on file and furnish them to the Government upon request.

4. **Statutory Restrictions Relating to Procurement Information.** [CONTRACTOR] acknowledges that certain Confidential Information may be subject to restrictions in Section 27 of the Office of Federal Procurement Policy Act (41 U.S.C. § 2104), as amended, and disclosures may result in criminal, civil, and/or administrative penalties. In addition, [CONTRACTOR] acknowledges that 18 U.S.C. § 1905, a criminal statute, bars an employee of a private sector organization from divulging certain confidential business information unless authorized by law.

5. **Limitations on Use of Confidential Information.** [CONTRACTOR] may obtain Confidential Information through performance of the Task Order orally or in writing. These disclosures or this access to information is being made upon the basis of the confidential relationship between the parties and, unless specifically authorized in accordance with this agreement, [CONTRACTOR] will:
   a) Use such Confidential Information for the sole purpose of performing the USCENTCOM support requirements detailed in the Task Order and for no other purpose;
   b) Not make any copies of Confidential Information, in whole or in part;
   c) Promptly notify GSA in writing of any unauthorized misappropriation, disclosure, or use by any person of the Confidential Information which may come to its attention and take all steps reasonably necessary to limit, stop or otherwise remedy such misappropriation, disclosure, or use caused or permitted by a [CONTRACTOR] employee.

6. **Duties Respecting Third Parties.** If [CONTRACTOR] will have access to the proprietary information of other companies in performing Task Order support services for the Government, [CONTRACTOR] shall enter into agreements with the other companies to protect their information from unauthorized use or disclosure for as long as it remains proprietary and refrain from using the information for any purpose other than that for which it was furnished. [CONTRACTOR] agrees to maintain copies of these third party agreements and furnish them to the Government upon request in accordance with 48 C.F.R. § 9.505-4(b).

7. **Notice Concerning Organizational Conflicts of Interest.** [CONTRACTOR] agrees that distribution, disclosure or dissemination of Confidential Information (whether authorized or unauthorized) within its corporate organization or affiliates, may lead to disqualification from participation in future Government procurements under the organizational conflict of interest rules of 48 C.F.R. § 9.5.

8. **Entire Agreement.** This Agreement constitutes the entire agreement between the parties and supersedes any prior or contemporaneous oral or written representations with regard to protection of Confidential Information in performance of the subject Task Order. This Agreement may not be modified except in writing signed by both parties.

9. **Governing Law**. The laws of the United States shall govern this agreement.

10. **Severability.** If any provision of this Agreement is invalid or unenforceable under the applicable law, the remaining provisions shall remain in effect.

In accordance with Public Law No. 108-447, Consolidated Act, 2005, the following is applicable:

> These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958; section 7211 of title 5, United States Code (governing disclosures to Congress); section 1034 of title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the

military); section 2302(b)(8) of title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including sections 641, 793, 794, 798, and 952 of title 18, United States Code, and section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive order and listed statutes are incorporated into this agreement and are controlling.

11. Beneficiaries. If information owned by an individual or entity not a party to this agreement is disclosed or misappropriated by [CONTRACTOR] in breach of this agreement, such information owner is a third party beneficiary of this agreement. However, nothing herein shall create an independent right of action against the U.S. Government by any third party.

IN WITNESS WHEREOF, GSA and [CONTRACTOR] have caused the Agreement to be executed as of the day and year first written above.

UNITED STATES GENERAL SERVICES ADMINISTRATION

_____ _____
Name Date

_____
Contracting Officer

[CONTRACTOR]

_____ _____
Name* Date

_____
Title

*Person must have the authority to bind the company.

ADDENDUM TO
NON-DISCLOSURE AGREEMENT
BETWEEN
U.S. GENERAL SERVICES ADMINISTRATION (GSA)
FEDERAL SYSTEMS INTEGRATION AND MANAGEMENT (FEDSIM)
AND [CONTRACTOR]

This agreement, made and entered into this _____ day of _____, 2010 (the "Effective Date"), is by and between GSA and [CONTRACTOR].

List of personnel (reference Section 2, Limitations on Disclosure, in Non-Disclosure Agreement):

1.
2.
3.
4.

IN WITNESS WHEREOF, GSA and [CONTRACTOR] have caused the Agreement to be executed as of the day and year first written above.

UNITED STATES GENERAL SERVICES ADMINISTRATION

_____ _____
Name Date
Contracting Officer

[CLIENT AGENCY]

_____ _____
Name Date
[CLIENT POC TITLE]

[CONTRACTOR]

_____ _____
Name Date
[CONTRACTOR POC TITLE]

Attachment F
Travel Authorization

TravelAuthorization0
8-04-11.xls

Attachment G
Removed for Award

Attachment H
Removed for Award

Attachment I

Quality Assurance Surveillance Plan (QASP)

QUALITY ASSURANCE SURVEILLANCE PLAN (QASP)

GSC-QFOB-12-XXXXX

USCENTCOM C4 Enterprise Support

IN SUPPORT OF:

United States Central Command

FEDSIM Project Number 11041DEM

1.0 INTRODUCTION

This Quality Assurance Surveillance Plan (QASP) is pursuant to the requirements listed in the Performance Work Statement (PWS) entitled USCENTCOM C4 Enterprise Support. This plan sets forth the procedures and guidelines USCENTCOM will use.

1.1 PURPOSE

The purpose of the QASP is to describe the systematic methods used to monitor performance and to identify the required documentation and the resources to be employed. The QASP provides a means for evaluating whether the Contractor is meeting the performance standards/quality levels identified in the PWS and the Contractor's Quality Control Plan (QCP), and to ensure that the government pays only for the level of services received.

This QASP defines the roles and responsibilities of all members of the Integrated Project Team (IPT), identifies the performance objectives, defines the methodologies used to monitor and evaluate the Contractor's performance, describes quality assurance documentation requirements, and describes the analysis of quality assurance monitoring results.

1.2 PERFORMANCE MANAGEMENT APPROACH

The PWS structures the acquisition around "what" service or quality level is required, as opposed to "how" the Contractor should perform the work (i.e., results, not compliance). This QASP will define the performance management approach taken by USCENTCOM to monitor and manage the Contractor's performance to ensure the expected outcomes or performance objectives communicated in the PWS are achieved. Performance management rests on developing a capability to review and analyze information generated through performance assessment. The ability to make decisions based on the analysis of performance data is the cornerstone of performance management; this analysis yields information that indicates whether expected outcomes for the project are being achieved by the Contractor.

Performance management represents a significant shift from the more traditional quality assurance (QA) concepts in several ways. Performance management focuses on assessing whether outcomes are being achieved and to what extent. This approach migrates away from scrutiny of compliance with the processes and practices used to achieve the outcome. A performance-based approach enables the Contractor to play a large role in how the work is performed, as long as the proposed processes are within the stated constraints. The only exceptions to process reviews are those required by law (federal, state, and local) and compelling business situations, such as safety and health. A "results" focus provides the Contractor flexibility to continuously improve and innovate over the course of the contract as long as the critical outcomes expected are being achieved and/or the desired performance levels are being met.

1.3 PEFORMANCE MANAGEMENT STRATEGY

The Contractor is responsible for the quality of all work performed. The Contractor measures that quality through the Contractor's own quality control (QC) program. QC is work output, not workers, and therefore includes all work performed under this contract regardless of whether the work is performed by Contractor employees or by subcontractors. The Contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. The Contractor will develop and implement a performance management system with processes to assess and report its performance to the designated government representative. The Contractor's QCP will set forth the staffing and procedures for self-inspecting the quality, timeliness, responsiveness, customer satisfaction, and other performance requirements in the PWS. This QASP enables the government to take advantage of the Contractor's QC program.

The government representative(s) will monitor performance and review performance reports furnished by the Contractor to determine how the Contractor is performing against communicated performance objectives. The government will make determination regarding incentives based on performance measurement metric data and notify the Contractor of those decisions. The Contractor will be responsible for making required changes in processes and practices to ensure performance is managed effectively.

2.0 ROLES AND RESPONSIBILITIES

2.1 Contracting Officer

The Contracting Officer (CO) is responsible for monitoring contract compliance, contract administration, and cost control and for resolving any differences between the observations documented by the Contracting Officer's Representative (COR), or Technical Point of Contact (TPOC) and the Contractor. The CO will designate one full-time COR as the Government authority for performance management. The number of additional representatives serving as technical inspectors depends on the complexity of the services measured, as well as the Contractor's performance, and must be identified and designated by the CO.

2.2 Contracting Officer Representative

The COR is designated in writing by the CO to act as his or her authorized representative to assist in administering a contract. COR limitations are contained in the written appointment letter. The COR is responsible for technical administration of the project and ensures proper government surveillance of the Contractor's performance. The COR is not empowered to make any contractual commitments or to authorize any contractual changes on the government's behalf. Any changes that the Contractor deems may affect contract price, terms, or conditions shall be referred to the CO for action. The COR will have the responsibility for completing QA monitoring forms used to document the inspection and evaluation of the Contractor's work performance. Government surveillance may occur under the inspection of services clause for any service relating to the contract

3.0 IDENTIFICATION OF REQUIRED PERFORMANCE STANDARDS/QUALITY LEVELS

The required performance standards and/or quality levels are included in the PWS and in Performance Requirements Summary in the Contractor's QC Plan. If the Contractor meets the required service or performance level, it will be paid the base fee amount agreed on in the Task Order. If the Contractor exceeds the service or performance level, it is eligible to receive an award fee as stated in the Task Order.

4.0 METHODOLOGIES TO MONITOR PERFORMANCE

4.1 Surveillance Techniques

In an effort to minimize the performance management burden, simplified surveillance methods shall be used by the government to evaluate Contractor performance when appropriate. The primary methods of surveillance are (include those that apply)

- Random monitoring, which shall be performed by the COR designated inspector.
- 100% Inspection – Each month, the COR, shall review the generated documentation and enter summary results into the Surveillance Activity Checklist.
- Periodic Inspection – COR typically performs the periodic inspection on a monthly basis.

4.2 Customer Feedback

The Contractor is expected to establish and maintain professional communication between its employees and customers. The primary objective of this communication is customer satisfaction. Customer satisfaction is the most significant external indicator of the success and effectiveness of all services provided and can be measured through customer complaints.

Performance management drives the Contractor to be customer focused through initially and internally addressing customer complaints and investigating the issues and/or problems but the customer always has the option to communicate complaints to the CO and/or the COR, as opposed to the Contractor.

Customer complaints, to be considered valid, must set forth clearly and in writing the detailed nature of the complaint, must be signed, and must be forwarded to the COR. The COR will accept those customer complaints and investigate using the Quality Assurance Monitoring Form – Customer Complaint Investigation, identified in Attachment 3.

Customer feedback may also be obtained either from the results of formal customer satisfaction surveys or from random customer complaints.

4.3 Acceptable Quality Levels

The Acceptable Quality Levels (AQLs) included in Attachment 1, Performance Requirements Summary Table, for Contractor performance are structured to allow the Contractor to manage

how the work is performed while providing negative incentives for performance shortfalls. For certain critical activities, the desired performance level is established at 100 percent. Other levels of performance are keyed to the relative importance of the task to the overall mission performance at USCENTCOM.

5.0 QUALITY ASSURANCE DOCUMENTATION

5.1 The Performance Management Feedback Loop

The performance management feedback loop begins with the communication of expected outcomes. Performance standards are expressed in the PWS and assessed using the performance monitoring techniques shown in paragraph 4.1.

5.2 Monitoring Forms

The Government's QA surveillance, accomplished by the COR, TPOC, or designated representative(s), will be reported using the monitoring forms in Attachments 2 and 3. The forms, when completed, will document the Government's assessment of the Contractor's performance under the contract to ensure that the required results (service and quality levels) are being achieved.

The COR will retain a copy of all completed QA surveillance forms.

6.0 ANALYSIS OF QUALITY ASSURANCE MONITORING RESULTS

6.1 Determining Performance

Government shall use the monitoring methods cited to determine whether the performance standards/service levels/AQLs have been met. If the Contractor has not met the minimum requirements, it may be asked to develop a corrective action plan to show how and by what date it intends to bring performance up to the required levels.

6.2 Reporting

At the end of each month, the COR will prepare a written report for the CO summarizing the overall results of the quality assurance surveillance of the Contractor's performance. This written report, which includes the Contractor's submitted monthly report and the completed quality assurance monitoring forms (Attachment 2), will become part of the QA documentation. It will enable the government to demonstrate whether the Contractor is meeting the stated performance standards.

6.3 Reviews and Resolution

The CO or COR may require the Contractor's project manager, or a designated alternate, to meet with the CO, COR, TPOC, or other Government IPT personnel as deemed necessary to discuss performance evaluation. The CO or COR will define a frequency of in-depth reviews with the

Contractor, including appropriate self-assessments by the Contractor; however, if the need arises, the Contractor will meet with the CO, COR, or TPOC as often as required or per the Contractor's request. The agenda of the reviews may include:

- Monthly performance assessment data and trend analysis
- Issues and concerns of both parties
- Projected outlook for upcoming months and progress against expected trends, including a corrective action plan analysis
- Recommendations for improved efficiency and/or effectiveness
- Issues arising from the performance monitoring processes.

The CO or COR must coordinate and communicate with the Contractor to resolve issues and concerns regarding marginal or unacceptable performance.

The COR, TPOC, and Contractor should jointly formulate tactical and long-term courses of action. Decisions regarding changes to metrics, thresholds, or service levels should be clearly documented. Changes to service levels, procedures, and metrics will be incorporated as a contract modification.

ATTACHMENT 1: PERFORMANCE REQUIREMENTS SUMMARY

The performance requirements contain a number of performance metrics across all task areas. Unless stated otherwise, all metrics shall be measured and reported on a monthly basis.

5.1 PMO Support Metrics for Monthly Period being measured

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Effectively manage cost				
Deliver Services within Cost Estimates	Meet Cost Target (This will exclude the Surge/EWW, Tools, Travel and ODC CLINS.)	Within 0% - + 5% of Estimated Cost	Financial Reports	Award Fee Determination: Positive Performance Evaluation
Metric B: Contract Staffing				
Staffing	Ability to maintain staffing during task order period.	92% - 96% overall staffing	Weekly or Daily staffing matrix reports.	Award Fee Determination: Positive Performance Evaluation
Metric C: Service Description: Accuracy of Staffing Matrix and CAC Requests				
Staffing Matrix and CAC Requests	Staffing matrix and CAC Requests will be maintained error free.	1 error per reporting period 0 = succeed 1 = met = or >2 = not met	Staffing and CAC Request repository	Award Fee Determination: Positive Performance Evaluation
Metric D: Service Description: Specified deliverables will be completed within the mutually agreed to timeframe.				
Deliverables per Section F – Task Area 1, Task 5.2 CONOPS, Task 5.4.2.4, Task 5.4.2.6, 5.6.1.1 and Task 5.6.3.1	Up-to-date and accurate within the mutually agreed to deadline – reported semi-annual	No more than 1 late > 5 days	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric E: Service Description: Customer Satisfaction				
Customer Satisfaction	Overall contract performance must remain within satisfactory range	Overall Rating of Good or Overall rating of Satisfactory	Aggregation of Monthly Scorecard performance	Award Fee Determination: Positive Performance Evaluation
Metric F: Service Description: Provide Extended Work Week (EWW) requests to GSA FEDSIM COR in a timely manner.				
EWW Requests	Submitted for GSA FEDSIM COR approval within 8 hours after receiving USCENTCOM CCJ6 Division level approval.	94% - 97% Compliance	EWW Repository	Award Fee Determination: Positive Performance Evaluation
Metric G: Service Description: Provide commercial airline flight Travel Authorization (TA) requests to GSA FEDSIM COR in a timely manner.				
TA Requests	1. Commercial airline flights shall be processed as follows: Priority 1 (travel w/i 2 days) – processed 1 business day after approval 2. Priority 2 (travel w/i 3 - 13 days) - processed within 2 days prior to departure date after approval 3. Priority 3 (travel > 13 days) – processed w/i 7 days prior to departure date (excluding weekends and holidays) (guarantees 7 day advance ticket purchase)	90% - 95% Compliance	Travel Repository	Award Fee Determination: Positive Performance Evaluation
Metric H: Service Description: Submit error-free invoices to the GSA FEDSIM COR.				
Invoice Submissions	Invoices submitted to the GSA FEDSIM COR for approval will be error-free. (Excludes requests for clarifications)	1 error or misrepresentation per month for invoice submissions	CostPoint	Award Fee Determination: Positive Performance Evaluation

5.2 – C4 Systems Support Metrics for Monthly Period being measured

C.5.2 CCJ6-S Division Level Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Division Level Availability of Core Services				
Maximize Availability	Ensure IT systems are accessible to users (including planned and unplanned outages)	98%-99% compliance within reporting period	Observation, EOC monitoring and reporting	Award Fee Determination: Positive Performance Evaluation
Metric B: Division Level Reliability of Core Services				
Maximize Reliability	Ensure IT systems are accessible to users except during planned outages	99.2%-99.7% compliance within reporting period	Observation, EOC monitoring and reporting	Award Fee Determination: Positive Performance Evaluation
Metric C: Priority 1 Users and Services				
Incident Resolution	Escalate or resolve incidents within 2 hours of submission	85%-90% compliance within reporting period	Remedy	Award Fee Determination: Positive Performance Evaluation

Metric D: Users and Services				
Incident Resolution (70%)	Resolve incidents within 24 hours of submission as measured daily	80%-90% compliance within reporting period	Remedy	Award Fee Determination: Positive Performance Evaluation
Metric E: Users and Services				
1-6 Day **Incident Resolution**	Resolve remaining (24 hour non-compliant) incidents within 6 days of submission as measured monthly	60%-75% compliance within reporting period	Remedy	Award Fee Determination: Positive Performance Evaluation

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric F: Execute DoD Level Security Directives				
Execute DoD Level Security Directives on time	Comply with all security directives from higher headquarters in the time specified in the directive (unless waived by USCENTCOM)	100% directives executed by suspense date (execution prior to suspense date is considered exceeded)	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric G: Priority 1 Service Requests				
Service Request Completion	Satisfy requests within 24 hours	85%-90% compliance within reporting period	Remedy	Award Fee Determination: Positive Performance Evaluation

Metric H: Service Requests				
Service Request Completion	Satisfy requests within seven days	85%-95% compliance within reporting period	Remedy	Award Fee Determination: Positive Performance Evaluation
Metric I: Customer Satisfaction				
Maximize User Satisfaction	Percentage of returned user surveys with a rating of "Good" or better	91%-96% within reporting period	Remedy	Award Fee Determination: Positive Performance Evaluation
Metric J: Service Description: Specified deliverables will be completed within the mutually agreed to timeframe.				
Deliverables per Section F – Task Area 2	Up-to-date and accurate within the mutually agreed to deadline	92% - 95% Compliance to deadlines	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

C.5.2.1.3 Patch and Test Facility Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Provide Tier 2 DISN System and Circuit Availability and Reliability				
Maintain Systems and Circuits in accordance with DISA Circular 310-130-2 and 300-175-9	Meet performance criteria depicted in reference circulars for inside plant communications circuits	Exceed performance criteria IAW DISA Circular 310-130-2 and 300-175-9 by 98% – 99%	FACIT	Award Fee Determination: Positive Performance Evaluation

C.5.2.2 Enterprise Network Services – Critical Services Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Critical Services Availability (i.e., AMHS, GCCS)				
Maximize Availability	Ensure IT systems are accessible to users (including planned and unplanned outages)	98%-99% compliance within reporting period	Reported outage log generated via Remedy/Email notification	Award Fee Determination: Positive Performance Evaluation
Metric B: Critical Services Reliability (i.e., AMHS, GCCS)				
Maximize Reliability	Ensure IT systems are accessible to users except during planned outages	99.2 – 99.7% compliance within reporting period	Reported outage log generated via Remedy/Email notification	Award Fee Determination: Positive Performance Evaluation

C.5.2.3.1 Visual Information Services

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Provide Successful VTC/AV Services				
Conduct successful VTC/AV events	Ensure no disruption to each VTC/AV event	99.2%-99.7% compliance within reporting period	Observation, EOC monitoring and VIS Reports	Award Fee Determination: Positive Performance Evaluation

C.5.2.4 Customer Support Operations Incident Resolution Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Call Abandonment Rate				
Call Abandonment Rate	**Respond to customers in a timely manner and provide effective service**	**Between 2%-3% abandoned calls**	**Automated Call Distribution (ACD) System**	Award Fee Determination: Positive Performance Evaluation

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric B: Call Wait in Queue				
Call Wait in Queue	Respond to customers in a timely manner and provide effective service	Average call wait time between 60-90 seconds	Automated Call Distribution (ACD) System	Award Fee Determination: Positive Performance Evaluation

C.5.2.5 Commander's Communications Team Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Testing and Packing Communications Equipment				
Proper testing and packing of communications equipment	Properly packed and tested mission equipment IAW approved test plan 37 - 48 hours prior to mission departure. (24 -36 hours – exceeds, 37 – 48 hours – met, and >49 hours and < 24 hours fails) (gear not available and < 60 hours of notification – does not count against this metric)	100% compliance within reporting period	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

C.5.2.6 Headquarters User Training Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Provide Quality Course Instructors				
Evaluate Instructor Performance	**Results of instructor surveys**	**Average survey score between 90-95% per course**	**Observation and exception reporting**	Award Fee Determination: Positive Performance Evaluation

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric B: Provide Quality Course Material				
Evaluate Course Material	Results of course surveys	Average survey score between 90-95%	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

5.3 – Network Operations Metrics for monthly period being measured

C.5.3.1 Level 1 Current Operations Fault Monitoring, Identification, and Resolution Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A Service Description: Tier 1 network event impact assessment.				
Network event impact assessment	Provide accurate network impacts	90% - 95% of accurate network impacts are provided	Impacts will be identified by the CCSD and/or equipment	Award Fee Determination: Positive Performance Evaluation
Metric B Service Description: Tier 1 network incident handling				
Acknowledgement or escalation of network incidents	Acknowledge or escalate incidents within 1 – 2 hours	90% - 95% compliance	Theater Remedy	Award Fee Determination: Positive Performance Evaluation

C.5.3.2 Theater Authorized Service Interruptions Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A Service Description: Authorized Service Interruptions (ASIs) impact assessment.				
Impact Assessment	Provide accurate network impacts	90% - 95% of accurate network impacts are provided	Impacts will be identified by the CCSD and/or equipment that is provided by requestor of the ASI	Award Fee Determination: Positive Performance Evaluation

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric B Service Description: Timeliness of ASI Processing Time				
ASI Processing	• ASIs with less than 100 CCSDs will be processed within 24 hours of receipt of official email request • ASIs with CCSDs between 101 and 400 will be processed within 48 hours of official email request • ASIs with CCSDs over 400 will be processed within 96 hours of official email request • Urgent ASI requests will take precedence over the above timelines and will be processed within 24 hours • Demand Maintenance ASI requests will take precedence over Urgent and Routine and will be processed and staffed within 12 hours of official email request	90% - 95% compliance processing Routine ASI request within allotted window based on size and status/urgency	Impacts will be identified by the CCSD and/or equipment that is provided by requestor of the ASI	Award Fee Determination: Positive Performance Evaluation

C.5.3.3 Deleted

5.4 – Engineering Support Metrics for monthly period being measured

5.4.1.2 – Project Management Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: Specified deliverables will be completed within the mutually agreed to timeframe.				
On-Time Deliverables	On-Time Deliverable compliance. This applies to all deliverables as specified in Section F of the TOR for Task Area 5.4.1.	≥90% compliance with approved schedules and within 80% of Project Management capacity	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric B: Service Description: Project schedules will be within 10% of plan.				
Schedule Variance	Maintain project schedules and meet mutually agreed to milestones.	Maintain schedule within 0%+ 10% of project plan and within 80% of Project Management capacity	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

5.4.2 – Engineering Design Analysis Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: Specified deliverables will be completed within the mutually agreed to timeframe.				
On-Time Deliverables	On-Time Deliverable compliance. This applies to all deliverables as specified in Section F of the TOR for Task	92% - 95% compliance with approved schedules	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric B: Service Description: Ensure timely response to Tier II support for Problem tickets escalated to Tier III (to include theater).				
Problem Ticket Response Time	Response to Tier II support for Problem tickets will occur within 1 business day of the problem ticket being escalated to Tier III. *** NOTE: This metric only applies to problem tickets that are processed through the approved Problem Management Process.*	94% - 96% compliance within reporting period	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

5.4.2.4 DELETED

5.4.2.5 DELETED

5.4.3 – Test, Analysis and Integration Lab Support Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: Specified deliverables will be completed within the mutually agreed to timeframe.				
Deliverables per Section F – Task Area 5.4.3	Up-to-date and accurate within the mutually agreed to deadline	92% - 95% compliance with approved schedules	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric B: Service Description: Information Assurance Vulnerability Alert (IAVA) patches shall be tested within the agreed timeframe.				
Test IAVA Patches	Timely testing of IAVA patches	94% - 96% compliance with approved schedules	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric C: Service Description: Ensure timely response to Tier II support for tickets escalated to Tier III.				
Problem Ticket Response Time	Response to Tier II support for Problem tickets will occur within 1 business day of the problem ticket being escalated to Tier III. *** NOTE: This metric only applies to problem tickets that are processed through the approved Problem Management Process.*	94% - 96% compliance within reporting period	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

5.4.4 – Software Engineering Support Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: Completion of change orders within the mutually agreed to timeframe.				
Change Order Completion	On time completion of change orders	94% - 96% compliance with approved schedules	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric B: Service Description: Software engineering documentation delivered within the mutually agreed to timeframe.				
Software documentation	Up-to-date and accurate	94% - 96% compliance with approved schedules	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

Metric C: Service Description: Maintain availability of web services assigned or designated to this Task Area.				
Web Service Availability	Percentage of web services availability	99.0 - 99.5% availability	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation:
Metric D: Service Description: Maintain availability of database services assigned or designated to this Task Area.				
Database Service Availability	Percentage of database services availability	99.0 - 99.5% availability	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation:

5.5 Cyber Security Metrics for monthly period being measured

5.5.1 – Headquarters Network Defense Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: Security incidents shall be reported and summarized to the EOC or TNC within 15 minutes after their detection.				
Security incident reporting	Reported within 15 minutes of detection	No more than 1 case per month where reporting is not done on time	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric B: Service Description: IAVA Compliance reports shall be published within 72 hours of a scan.				
IAVA Compliance	Up-to-date and accurate within 72 hours of a scan	No more than 1 case per month where reporting is not done on time	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric C: Service Description: Customer contact shall occur for all tickets within 24 business hours of assignment.				
Trouble Tickets (service requests)	Establish customer contact within 24 business hours of ticket assignment.	94% - 96% compliance	Observation, customer feedback	Award Fee Determination: Positive Performance Evaluation

5.5.2 – Theater Cyber Initiatives Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: Assessments are completed within prescribed timelines.				
Program assessment	Up-to-date and accurate	94% - 96% accomplished within prescribed timelines.	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric B: Service Description: Respond to requests for information from components promptly.				
RFI response	Contact with customer within 3 working days.	94% - 96% compliance with standard.	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric C: Service Description: Thorough analysis of findings from theater/AOR assessments.				
Findings Analysis	Thorough, accurate, and complete.	94% - 96% reporting within prescribed timelines.	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

5.5.3 – Cyber Certification and Accreditation Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: The initial review of Authority to Connect (ATC) documentation shall be completed within three business days.				
Review of ATC documentation	Up-to-date and accurate within 3 business days	94% - 96% ATCs reviewed within standard.	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric B: Service Description: Correct request for ATC shall be forwarded to DISA within two business days.				
Forward correct request for ATC to DISA	Up-to-date and accurate within 2 business days	94% - 96% ATCs forwarded within standard.	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric C: Service Description: Authority to Operate (ATO) shall be completed within a mutually agreed to deadline.				
ATO completion	Timeliness by mutually agreed to deadline	94% - 96% ATOs completed before deadline.	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric D: Service Description: Interim Authority to Operate (IATO) shall be completed within a mutually agreed to deadline.				
IATO completion	Timeliness by mutually agreed to deadline	94% - 96% IATOs completed before deadline.	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric E: Service Description: Interim Authority to Test (IATT) shall be completed within a mutually agreed to deadline.				
IATT completion	Timeliness by mutually agreed to deadline	94% - 96% IATTs completed within standard.	Remedy and observation, customer feedback	Award Fee Determination: Positive Performance Evaluation

Table 48 – Active Cyber Defense Metrics:

Performance Objective	Performance Standard	AQL (by Priority)	Monitoring Method	Incentive
Metric A: Service Description: Security incidents shall be reported and summarized to the Cyber Security Division Leadership within 60 minutes after their detection.				
Security incident reporting	Up-to-date and accurate within 15 minutes of detection	No more than 1 case per month where reporting is not done on time	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation:
Metric B: Service Description: Assessments are completed within prescribed timelines.				
Perform Program Assessments	Deliver DRAFT program assessment within 48 hours of acceptance	No more than 2 assessments per month delivered after the 48 hour time period	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation:
Metric C: Service Description: Collect and analysis computer and network forensics within 60 hours.				
Perform	Deliver full	No more than 1	Observation and	Award Fee

Forensics Assessments	forensics assessment within 60 hours	assessments per month delivered after the 60 hour time period	exception reporting	Determination: Positive Performance Evaluation:

5.6 Programs and Architectures Support Metrics for monthly period being measured

5.6.1.1 - Deleted

5.6.1.2 - Deleted

5.6.2 – Service Transition Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: Timely updates to the Configuration Management Database.				
CMDB Updates	Hardware within 3 working days of task assignment Software within 5 working days of task assignment Contracts within 10 working days of task assignment Services within 5 working days of task assignment	90% - 95% Compliance	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

5.7 Resource Management Support Metrics for Monthly Period being measured

5.7.1 – Resource Management Support Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: Process Command Records.				
Processed Records	Process on average 200,000 records	94% - 96% compliance	TRIM monthly report	Award Fee Determination: Positive Performance Evaluation
Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric B: Service Description: Requested desk-side TRIM training shall be performed in a timely manner.				
Desk-side TRIM training performed	Requested desk-side TRIM training will be performed within 3 business days of request.	94% - 96% compliance	TRIM monthly report	Award Fee Determination: Positive Performance Evaluation

5.7.2 – Asset Management Support Metrics

Performance Objective	Performance Standard	AQL	Monitoring Method	Incentive
Metric A: Service Description: CFH Information Technology Asset accountability shall be maintained.				
Accountability CFH IT inventory	Maintain accountability of CFH inventory	94% - 96% accountability	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation
Metric B: Service Description: Accurately maintain data pertaining to received and disposed assets.				
Accurately maintain asset data.	Asset data will be accurately annotated through the process of receiving and disposing of ordered assets.	90% - 95% accuracy of assets data correctly annotated	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation

5.7.3 – Knowledge Management Support Metrics

Performance Objective	Performance Standard	AQL (by Priority)	Monitoring Method	Incentive
Metric A: Service Description: Provide all deliverables as specified in Section F of this TOR for Task on time and accurate within the mutually agreed to deadline.				
Knowledge Management Deliverables	Up-to-date and accurate within the mutually agreed to deadline	≥95% Compliance to deadlines	Observation and exception reporting	Award Fee Determination: Positive Performance Evaluation:
Metric B: Service Description: KIMB/KIMWG/JKIMWG Execution				
Efficient and effective execution for KM governance	KM board facilitation documentation developed within agreed to timeframe	95 % compliance of deadlines	Observation and exception reporting Award Fee Determination:	Positive Performance Evaluation:

ATTACHMENT 2

SAMPLE QUALITY ASSURANCE MONITORING FORM

SERVICE or STANDARD: _____

_____

_____

_____

_____

SURVEY PERIOD: _____

SURVEILLANCE METHOD (Check):

❒ Random Sampling ❒ 100% Inspection ❒ Periodic Inspection ❒ Customer Complaint

LEVEL OF SURVEILLANCE (Check):

❒ Monthly ❒ Quarterly ❒ As needed

PERCENTAGE OF ITEMS SAMPLED DURING SURVEY PERIOD: _____ %

ANALYSIS OF RESULTS:

Observed Service Provider Performance Measurement Rate: _____%

Service Provider's Performance (Check): ❒ Meets Standards

❒ Does Not Meet Standards

Narrative of Performance During Survey Period: _____

_____

_____

_____

_____

PREPARED BY: _____ **DATE:** _____

ATTACHMENT 3

QUALITY ASSURANCE MONITORING FORM – CUSTOMER COMPLAINT INVESTIGATION

SERVICE or STANDARD:
_____
_____
_____

SURVEY PERIOD: _____

DATE/TIME COMPLAINT RECEIVED: _____ _____ AM / PM

SOURCE OF COMPLAINT: _____ (NAME)
_____ (ORGANIZATION)
_____ (PHONE NUMBER)
_____ (EMAIL ADDRESS)

NATURE OF COMPLAINT:
_____
_____
_____
_____

RESULTS OF COMPLAINT INVESTIGATION:
_____
_____
_____
_____

DATE/TIME SERVICE PROVIDER INFORMED OF COMPLAINT: _____ _____ AM / PM

CORRECTIVE ACTION TAKEN BY SERVICE PROVIDER:
_____
_____
_____
_____

RECEIVED AND VALIDATED BY: _____

PREPARED BY: _____ **DATE:** _____

Attachment J

Acronym List

AAR	After Action Report
ADP	Automated Data Processing
ADPE	Automated Data Processing Equipment
ADUA	Administrative Directory User Agent
AEF	Air and Space Expeditionary Force(s)
AFB	Air Force Base
AFDO	Award Fee Determining Official
AFDP	Award Fee Determination Plan
AFEB	Award Fee Evaluation Baord
AFI	Air Force Instruction
AFMAN	Air Force Manual
AFP	Award Fee Period
AIS	Automated Information Systems
AMHS	Automated Message Handling System
ANSI	American National Standards Institute
AOR	Area of Responsibility
AQL	Acceptable Quality Level
ASI	Authorized Service Interruption
ASP	Active Server Page
ASR	Aggregation Service Routers
ATM	Asynchronous Transfer Mode
AUTODIN	Automatic Digital Information Network
A/V	Audio-Visual
AWACS	Airborne Warning and Control System
BGP	Border Gateway Protocol
BICSI	Building Industry Consulting Service International
C&A	Certification and Accreditation
C2	Command and Control
C2PC	Command and Control Personal Computer
C4	Command, Control, Communications, and Computers
CA	Certificate/Certification Authority
CAB	Change Advisory Control Board
CAC	Common Access Card
CAF	Contract Access Fee
CAFRO	Client Award Fee Recommending Official
CAP	Command Automation Plan/Program
CAW	Certificate Authority Workstation
CCB	Configuration Control Board
CCER	CENTRIXS Cross Enclave Requirement
CCIE	CISCO Certified Internetwork Expert
CCIR	Commander’s Critical Information Requirement
CCJ6	U.S. Central Command C4 Directorate

CCNA	CISCO Certified Network Administrator/Associate
CCNP	CISCO Certified Network Professional
CCP	Contingency Communications Package
CCR	USCENTCOM Regulation
CCTO	USCENTCOM Communications Tasking Order
CCTV	Closed Circuit Television
CD	Compact Disc
CDI	Conditioned Diphase
CD-ROM	Compact Disk-Read Only Memory
CDS	Cross Domain Solution
CEB	CIO Executive Board
CENTRANET	U.S. Central Command Intranet, SECRET
CENTRIXS	Combined Enterprise Regional Information Exchange System
CERP	Computer Equipment Replacement Program
CFACC	Combined Force Air Component Commander/Command
CFH	Contingency Forward Headquarters/USCENTCOM Forward Headquarters
CFLCC	Combined Force Land Component Commander/Command
CFMCC	Combined Force Maritime Component Commander/Command
CFR	Code of Federal Regulations
CI	Configuration Item
CINCCENT	Commander-in-Chief, U.S. Central Command
CIO	Chief Information Officer
CISSP	Computer Information Systems Security Professional
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJTF	Coalition Joint Task Force
CLIN	Contract Line Item Number
CMDB	Configuration Management DataBase
CND	Computer Network Defense
CO	Contracting Officer
COA	Course(s) of Action
COCOM	Combatant Command
COE	Common Operating Environment
COMSEC	Communications Security
COMUSAFCENT	Commander, U.S. Central Air Forces
COMUSARCENT	Commander, U.S. Army Central
COMUSMARCENT	Commander, U.S. Marine Forces Central
COMUSNAVCENT	Commander, U.S. Naval Forces Central
CONOPS	Concept of Operations
CONUS	Continental United States
COOP	Continuity of Operations
COP	Common Operational Picture
COR	Contracting Officer’s Representative
TPOC	Technical Point of Contact
COTS	Commercial Off-The-Shelf
CPAF	Cost-Plus-Award-Fee

CPN	USCENTCOM Partner Network
CPU	Central Processing Unit
CPXP	CommPower's XML Portal
CR	Customer Request
CRO	COMSEC Responsible Officer
CSD	Common SIPR Domain
CSO	Customer Support Operations
CSS	Cascading Style Sheets
CSU	Channel Service Unit
CTOs	Communication Tasking Orders
CTP	Consent to Purchase
CXI	CENTRIXS
DAA	Designated Approval Authority
DADS	DII Assets Distribution System
DARS	DoD Architecture Repository System
DCO	Defense Collaboration Online
DEPORD	Deployment Order
DFAR	Defense Federal Acquisition Regulation
DHCP	Dynamic Host Configuration Protocol
DHL	Definitive Hardware Library
DIACAP	DoD Information Assurance Certification and Accreditation Process
DII	Defense Information Infrastructure
DIO	Defensive Information Operations
DISA	Defense Information Systems Agency
DISAC	Defense Information Systems Agency Circular
DISN	Defense Information System Network
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DM	Data Management
DMS	Defense Messaging System
DMS-AF	Defense Messaging System – Air Force
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DoDI	Department of Defense Instruction
DRMO	Defense Reutilization Management Office
DRSN	Defense Red Switch Network
DSA	Directory Service Agent
DSG	Director's Strategy Group
DSL	Definitive Software Library
DSN	Defense Switched Network
DSSR	Department of State Standardized Regulations
DSU	Data Service Unit
DSWAG	Defense System Acquisition Working Group
DVD	Digital Video Disk
DVS	Defense Video Services
EA	Enterprise Architecture
EHF	Extremely High Frequency

EIE	Enterprise Information Environment
EIGRP	Enhanced Interior Gateway Routing Protocol
EIT	Electronic and Information Technology
EKMS	Electronic Key Management System
eMASS	Enterprise Mission Assurance Support Service
EOC	Enterprise Operations Center
ESG	Expeditionary Strike Group
ET	Eastern Time
EVM	Earned Value Management
FAR	Federal Acquisition Regulation
FCB	Functional Capabilities Board
FEDSIM	Federal Systems Integration and Management
FEN	Field Engineering Notes
FER	Firewall Exception Requests
FISMA	Federal Information Systems Management Act
FM	Functional Manager
FMN	Future Mission Network
FO	Flag Officer
FOIA	Freedom of Information Act
FoS	Family of System
FTR	Federal Travel Regulation
FY	Fiscal Year
GAR	Gateway Access Request
GBS	Global Broadcast Service
GCCS	Global Command and Control System
GCCS-A	Global Command and Control System - Army
GCCS-AF	Global Command and Control System – Air Force
GCCS-J	Global Command and Control System – Joint
GCCS-M	Global Command and Control System - Marines
GCED	GIAC Certified Enterprise Defender
GCTF	Global Counterterrorism Force
GCWN	GIAC Certified Windows Security Administrator
GETS	Government Emergency Telecommunications Service
GFE	Government-Furnished Equipment
GFI	Government-Furnished Information
GFP	Government Furnished Property
GIAP	Government Interconnection Approval Process
GIG	Global Information Grid
GM	Group Manager
GO	General Officer
GOTS	Government Off-The-Shelf
GSA	General Services Administration
GSAM	General Services Administration Acquisition Manual
GSM	Global Secure Mobile
HAZCON	Hazardous Condition
HBSS	Host-Based Security System

HQ	Headquarters
HSRP	Hot Standby Router Protocol
HTML	HyperText Markup Language
http	hyper text transfer protocol
I3	Integrated Imagery and Intelligence
IA	Information Assurance
IA/CND	Information Assurance/Computer Network Defense
IAM 2	Information Assurance Management Level 2
IAM	Information Assurance Manager/Management
IAT 1	Information Assurance Technical Level 1
IAT 2	Information Assurance Technical Level 2
IAT 3	Information Assurance Technical Level 3
IAVA	Information Assurance Vulnerability Alert
IAVM	Information Assurance Vulnerability Management
IAW	In Accordance With
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
INFOCON	Information Operations Condition
INFOSEC	Information Systems Security
IO	Information Operations
IP	Internet Protocol
IPL	Integrated Priority List
IPT	Integrated Project Team
IRM	Information Resource Management
IS	Information Systems
ISAF	International Security Assistance Force
ISDN	Integrated Services Digital Network
ISR	Intelligence, Surveillance, Reconnaissance
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITLM	Information Technology Life Cycle Management
IT PfM	Information Technology Portfolio Management
ITSM	Information Technology Service Management
J6	Joint Command and Control, Communications, and Computer Systems Directorate
JACAE	Joint Command and Control Architecture Capabilities Assessment Environment
JC2	Joint Command and Control
JCA	Joint Capability Area
JCET	Joint Combined Exchange Training
JCIDS	Joint Capabilities Integration Development System
JCPAT-E	Joint C4I Program Assessment Tool - Empowered
JCS	Joint Chiefs of Staff
JFACC	Joint Force Air Component Commander
JFLCC	Joint Force Land Component Commander
JFMCC	Joint Force Maritime Component Commander
JNO	Joint Net-Centric Operations

JOPES	Joint Operation Planning and Execution System
JPAS	Joint Personal Adjudication System
JS	Joint Staff
JTF	Joint Task Force
JTR	Joint Travel Regulations
JUONS	Joint Urgent Operational Needs Statement
JWICS	Joint Worldwide Intelligence Communications System
KM	Knowledge Management
KPI	Key Performance Indicators
LAN	Local Area Network
LCR	Life Cycle Replacement
MAGTF	Marine Air Ground Task Force
MAJCOM	Major Command
MARCENT	U.S. Marine Corps Central Command
MCFI	Multinational Coalition Force-Iraq
MCITP	Microsoft Certified Information Technology Professional
MCSA	Microsoft Certified Systems Administrator
MCSE	Microsoft Certified Solutions Expert/Systems Engineer
MCU	Multipoint Control Unit
MEU SOC	Marine Expeditionary Unit Special Operations Capable
MNIS	Multi-National Information Sharing
MOA	Memorandum of Agreement(s)
MOSS	Microsoft Office SharePoint Server
MOUS	Microsoft Office User Specialist
MPC	Military Payment Certificate
MS	Microsoft
MSEL	Master Scenario Events List
MSL	Master Station Log
MSO	Maritime Security Operations
MSR	Monthly Status Report
MYSQL	My Structured Query Language
NECA	National Electric Contractors Association
NetOps	Network Operations
NI	Network Infrastructure
NIPRNet	Non-secure Internet Protocol Router Network
NLT	No Later Than
NOC	Network Operations Center
NSA	National Security Agency
NSA	Naval Support Activity
NSTISSI	National Security Telecommunications and Information Systems Security Incident
NTE	Not-to-Exceed
O&M	Operations and Maintenance
OASD(NII)	Office of the Assistant Secretary of Defense (Networks and Information Integration)
OCONUS	Outside the Continental United States

ODC	Other Direct Costs
ODM	Operational Directive Message
OEF	Operation Enduring Freedom
OIF	Operation Iraqi Freedom
OMB	Office of Management and Budget
OND	Operation New Dawn
OPSEC	Operational Security
OPT	Operational Planning Team
OSD	Office of the Secretary of Defense
PA	Public Address
PBSC	Performance Based Services Contracting
PBX	Private Branch Exchange
PC	Personal Computer
PDA	Personal Digital Assistant
PEDs	Portable Electronic Devices
PfM	Portfolio Management
PHP	Hypertext Preprocessor
PKI	Public Key Infrastructure
PM	Performance Monitor
PMC	Project Management Charters
PMI	Preventive Maintenance Inspection(s)
PMO	Program Management Office
PMP	Project Management Plan
PMP	Project Management Professional
PNR	Problem Notification Report
POC	Point of Contact
POM	Program Objective Memorandum
POTS	Plain Old Telephone System
PPSM	Ports, Protocols, and Services Management
PTF	Patch and Test Facility
PWCS	Personal Wireless Communications Manager
PWS	Performance Work Statement
QASP	Quality Assurance Surveillance Plan
QC	Quality Control
QCP	Quality Control Plan
QOS	Quality of Service
REL A	Releasable to US, UK, Australia, Canada
RF	Radio Frequency
RFC	Request For Change
RFF	Request for Forces
RFI	Request for Information
RFS	Request for Services
RIM	Research in Motion
RIP	Relieve in Place
RIP	Request to Initiate Purchase
RIP/TOA	Relief In Place / Transfer of Authority

ROI	Return On Investment
SABI	Secret and Below Interoperability
SAN	Storage Area Networks
SAO	Security Assistance Office
SAR	Satellite Access Request
SATCOM	Satellite Communications
SCCM	System Center Configuration Manager
SCI	Sensitive Compartmented Information
SCO	Security Cooperation Organization
SCOM	System Center Operations Manager
SDD	Software Design Documents
SHADE	Shared Data Environment
SHF	Super High Frequency
SIPR	Secret Internet Protocol Router
SIPRNet	Secret Internet Protocol Router Network
SKL	Simple Key Loader
SLA	Service Level Agreement
SMART	Secure Messaging and Remote Terminal
SMCCS	Secure Mobile Cellular Communications System
SME PED	Secure Mobile Environment Portable Electronic Device
SME	Subject Matter Expert
SNAP	Standard Network Access Protocol
SNMP	Simple Network Management Protocol
SOCCENT	Special Operations Command, Central
SOFA	Status of Forces Agreement
SONET	Synchronous Optical Network
SOP	Standard Operating Procedure
SOW	Statement of Work
SPECAT	Special Category
SQL	Standard Query Language
SSBI	Single Scope Background Investigation
SSBI-PR	Single Scope Background Investigation – Periodic Review
SSO	Special Security Office
STE	Secure Telephone Equipment
STG	Strategic Technical Guidance
STIG	Security Technical Implementation Guide
SUE	Small Unit Exchange
SWarF	Senior Warfighters' Forum
TAMD	Theater Air Missile Defense
TBMCS	Theater Battle Management Core System
TCO	Telephone Control Officer(s)
TDM	Time Domain Multiplexer
TEB	Technical Evaluation Board
TIG	Theater Information Grid
TMAP	Telecommunications and Monitoring Assessment Program
TMF	Tivoli Management Framework

TMS	Ticket Management System
TMT	Task Management Tool
TNC	Theater NetOps Center
TNC	Theater Network Center
TNMA	Theater Network Management Architecture
TO	Task Order
TOA	Transfer of Authority
TOA	Task Order Award
TOMP	Task Order Management Plan
TOR	Task Order Request
TOS	Tracking and Ordering System
TRIM	Total Records and Information Management
TS	Top Secret
TS/C	Top Secret Collateral
TS/SCI	Top Secret/Sensitive Compartmented Information
TTP	Tactics, Techniques, and Procedures
U.S.	United States
UDOP	User Defined Operational Picture
UHF	Ultra High Frequency
UK	United Kingdom
UNIX	Unix Operating System
USA	United States Army
USAF	United States Air Force
USAFCENT	U.S. Air Forces Central Command
USARCENT	U.S. Army Forces Central Command
USC	United States Code
USCENTCOM	United States Central Command
USCYBERCOM	United States Cyber Command
USCINCCENT	Commander-in-Chief, U.S. Central Command
USFI	United States Forces - Iraq
USMARCENT	U.S. Marine Forces Central Command
USMC	U.S. Marine Corps
USN	U.S. Navy
USNAVCENT	U.S. Naval Forces Central Command
VA	Virginia
VB	Visual Basic
VIP	Very Important Person
VIS	Visual Information Services
VOIP	Voice Over Internet Protocol
VOSIP	Voice Over Secure Internet Protocol
VPN	Virtual Private Network
VSS	Virtual Switching System
VTC	Video Teleconference
WAN	Wide Area Network
WARNORD	Warning Order

WBS	Work Breakdown Structure
WMD	Weapon(s) of Mass Destruction
WO	Work Order
www	Worldwide Web

Attachment K
Problem Notification Report

PROBLEM NOTIFICATION REPORT

TASK ORDER NUMBER: _____ DATE: _____

1. Nature and sources of problem:

2. TPOC was verbally notified on: (date) _____

3. Is action required by the Government? Yes_____ No_____

4. If YES, describe Government action required and date required:

5. Will problem impact delivery schedule? Yes_____ No_____

6. If YES, identify what deliverables will be affected and extent of delay:

7. Can required delivery be brought back on schedule? Yes_____ No_____

8. Describe corrective action needed to resolve problems:

9. When will corrective action be completed?

10. Are increased costs anticipated? Yes_____ No_____

11. Identify amount of increased costs anticipated, their nature, and define Government responsibility for problems and costs:

Attachment L
Attachment deleted

Attachment M
Consent to Purchase

Attachment M – Consent to Purchase Template

Consent to Purchase

Date – DD-Mmm-YY
CTP# CC0000X
Prepared for: USCENTCOM CCJ6
Quote Expires – DD-Mmm-YY

DESCRIPTION	UNITS	PRICE	EXTENDED
Insert Product Description Here			
Insert Product Description Here			
Insert Product Description Here			
Insert Product Description Here			
		Fixed Fee	
		Total	

Total Quote - $

Pricing is only valid through the CCJ6 Team (TBD) (Insert Industry Partner Name Here Contract # GS00T99ALDXXXX Order # GS-T0008AJM088

FirstName LastName
Job Title
Industry Partner
USCENTCOM CCJ6-Team (TBD)
813.827.XXXX (w)
813.XXX.XXXX(f)
Email Address

Approved by:_____ Date:_____

Attachment N
Regulations and Publications

This attachment is divided into two sections based on their accessibility: GREEN: Accessible via the internet either in a commercial, .mil or .gov domain. RED: Accessible via internal USCENTCOM SIPRnet domain. These documents will be available to read while on a USCENTCOM SIPRnet machine in Tampa, FL. The vendor shall contact the FEDSIM Contracting Officer and Contract Specialist to request viewing of these publications. Most publications in this grouping do not require a Secret Clearance to review unless highlighted with the following, *Secret Clearance Required*. The vendor shall forward the name of the designated personnel with the applicable clearance (as required) for viewing the requested publications. A minimum of 24-hours' notice is required for the USCENTCOM Security Office to make appropriate coordination for reviewing the requested publications.

C.5.1 PMO Support

- Theater Business Clearance (TBC) applies to all contracts with performance in the CENTCOM Area of Responsibility (AOR)
- Deputy USD Memo, TBC-CAD Compliance, 15 Sep 09
- DPAP Memo, TBC-CAD Update, 29 Jun 10
- DPAP Memo, TBC-CAD Update, 13 Oct 10
- Contract Coordination in the CENTCOM AOR, 22 Nov 10
- C3 Commanders Critical Information Requirements Report- CCIR, Sep 10
- TBC Iraq Afghanistan
- Contracting Officers' Guide for Theater Business Clearance, Iraq-
- Afghanistan, Revised 15 Oct 11
- TBC Request and Tracker – Iraq Afghanistan 15 Oct 11
- PGI 225.74 Defense Contractors Outside the US
- DFARS 225.74, DFARS/PGI view)
- PGI 225.7401 Contracts requiring performance or delivery in a foreign country
- CENTCOM-Joint Theater Support Contracting Command (C-JTSCC) is the designated approval authority exercising TBC for Iraq, Afghanistan, Kuwait and Pakistan
- Synchronized Predeployment and Operational Tracker (SPOT): The Department of Defense (DoD) implemented SPOT as the single source to track deployed contractor personnel supporting DoD military operations worldwide
- SPOT DFARS Deviation 2007-0004, 19 Mar 07
- OUSD (AT&L), SPOT Implementation Guidance, DPAP, 28 Jan 08
- OUSD (AT&L), Policy on the Transition to and Use of an Automated Census, 19 Jan 10
- SPOT FRAGO 09-1451
- SPOT FRAGO 09-1451 Mod 2
- SPOT Class Deviation 2007-000010
- SPOT plus Memo, 6 Jan 11
- SPOT Transition Memo, 20 Jan 10
- SPOT Plus Census User Guide, 1 Feb 11

- SPOT Business Rules, 7 Sep 10
- Joint Publication 4-10, Operational Contract Support
- DODI 3020.50, Private Security Contractors Operating in Contingency Operations
- DODI 3020.41, Contractor Personnel Authorized to Accompany the US Armed Forces
- Procurement Roles and Responsibilities – GSO (Depart of State) and DoD Personnel
- US Code 10 USC Sec 101, Definitions – Contingency
- C-JTSCC Acquisition Instruction (AI)
- C-JTSCC AI Appendix 2—Part 52 Clauses
- Defense Contingency Contracting Handbook
- CENTCOM-Joint Theater Support Contracting Command (C-JTSCC)

C.5.2 C4 Systems Support

- USCENTCOM Regulation 12-2, (Information Resource Management), 17-Jan-2007.
- USCENTCOM Regulation 25-206, (Network Operations), 21-Sep-2007.
- USCENTCOM Regulation 105-12, Video Teleconference Program, 17-Dec-2007.
- USCENTCOM Regulation 380-8 (Automated Information Systems (AIS) Security Program), 20-Aug-2001.
- USCENTCOM Regulation 525-31, Hurricane Preparedness Standing, 08-Nov-2007.
- Office of Management and Budget (OMB) Circular A-130.
- CCR 310-3, Reproduction, Printing, Duplicating and Copying, 28-Sep-2006.
- USCENTCOM Regulation 37-13, (Internal Management Control Program), 01-Apr-1998.
- USCENTCOM Regulation 12-2, Security Assistance Policy, Administration and Management, 27-Jun-2002.
- USCENTCOM Regulation 25-61, USCENTCOM Mail Procedures, 26-Sep-2000.
- USCENTCOM Regulation 25-22, U.S. Central Command Global Command And Control System Program Instruction, 15-Jan-2002.
- USCENTCOM Regulation 25-50, Information Management Records Management Policy.
- CCR 10-2 USCENTCOM Organization and Functions.
- Chairman of the Joint Chiefs of Staff Manual CJCSIM 6231 series, Manual for Employing Joint Tactical Communications, 17-Nov-2000.
- DISA Circular 310-55-1, Status Reporting for DCS, 21-Jan-2000.
- DISA Circular 310-70-1, DII Technical Control, 25-Jun-1998.
- DISA Circular 310-70-57, DII Quality Assurance Program, 13-Apr-1998.
- DISA Circular 300-175-9, DII Operating-Maintenance Electrical Performance Standards, 08-Jun-1998.
- DoD Instruction (DoDI) 5200.40, 30-Dec-1997.
- DoDI 8510.1-M, 28-Nov-2007.
- All COMSEC directives in the following: AFI 33-215 (01-Jan-1998); and AFI 33-210.
- AFI 33-211 (01-Oct-1999), http://www.fas.org/irp/DoDdir/usaf/33-211.htm
- USCENTCOM Regulation 25-105, Forms Management Program, 02-Feb-2007.

- CCJ6 Network Operations Center Standard Operating Procedure #NOC 02-011, 22-Jul-2002.
- AFI 33-209.

C.5.2.1.1 Management of HQ Systems Infrastructure

- DISAC 300-115-3, Defense Information System Network (DISN) Secret Internet Protocol Routing Network (SIPRNet) Security Classification Guide, 25 October 2007.
- DoD Instruction (DoDI) 8110.1, MultiNational Information Sharing Networks Implementation, 06-Feb-2004.
- DISAC 630-125-1, **Net**-Centric Review Process, 6 October 2006.
- DISAC 300-110-2**,** World Wide On-Line System-Replacement and Defense Information System Network-Integrated Information Security Classification Guide, 02-June-1998.
- AFI 33-115, Volume 1, Network Operations (NetOps), 24-May-2006.
- CENTCOM Regulation (CCR) 105-13, USCENTCOM Information Operations Conditions, 10-Dec-1999.
- CJCSI 6510.01D, Information Assurance (IA) and Computer Network Defense (CND), 15-Aug-2007.

C.5.2.1.2 Voice Services

- Air Force Instruction 33-111, 05-Nov-2007.
- Air Force Instruction 33-220, On-Hook Telephone Security, 21-Nov-2007.
- USCENTCOM Regulation 37-13, Internal Management Control Program.
- CENTCOM Publication 105-7, Voice Communication Services, 16-May2005.
- MacDill Instruction 33-104, Base Telephone Service, http://www.e-publishing.af.mil/shared/media/epubs/MACDILLAFBI33-104.pdf.
- Voice & Video over Internet Protocol STIG Version 3, Release 2

C.5.2.1.3 Patch and Test Facility Support

- DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards, 24 July 2006.
- DISAC 310-70-1, DII Technical Control, 8 May 2006.
- DISAC 310-70-S1, DII Technical Control Test Descriptions, 8 May 2002.
- DISAC 310-55-1, Status Reporting, 8 May 2002.
- DISAC 310-55-9, Base Level Support for the Defense Information System Network (DISN), 12 July 2006.
- DISAC 310-65-1, Circuit and Trunk File Data Elements and Codes Manual of the Global Information Grid (GIG), 25 May 2006.
- DISAC 310-70-57, DII Quality Assurance Program, 21 April 2006.
- DISAC 310-130-1, Submission of Telecommunications Service Requests, 25 May 2006.
- DISAC 310-130-2, Management Thresholds and Performance Objectives, 21-Apr-2000
- Air Force Instruction 33-116, Long-Haul Telecommunications Management.
- AFMAN 23-110, Basic USAF Supply Manual.
- CCJ6-D Cable Labeling Standards SOP.

C.5.2.1.4 Cable Plant Support

- NSTISSAM TEMPEST/2-95 12 December 1995; RED/BLACK INSTALLATION GUIDANCE.

C.5.2.2.1 Communications Center

- Air Force Instruction 33-113, Communication and Information Telephone, Managing Air Force Message Centers, 06-Feb-2007.
- Air Force Instruction 33-129, Communication and Information, Web Management and Internet Use, 03-Feb-2005.
- Air Force System Security Instruction 3034, Communication and Information, FORTEZZA User Information.
- Air Force Instructions 33-201V1-5, 9, Communication and Information, Communication Security (COMSEC), http://www.e-publishing.af.mil.
- X509 Certificates Policy for the United States Department of Defense, also found on http://iase.disa.mil/pki/DoD-cp-v90-final-9-feb-05-signed.pdf.
- Communications and Electronics TELECOMMUNICATIONS SERVICES R 105-3.
- Communications and Electronics SECURITY ASSISTANCE ORGANIZATION (SAO) COMMUNICATIONS-ELECTRONICS MAINTENANCE R 105-8.
- CCR 380-14 Security Classification Guide 0501, 27-Sep-199.6
- Air Force Instruction 33-277, Communication and Information, FORTEZZA Operational Security, http://www.e-publishing.af.mil/shared/media/epubs/AFI33-277.pdf.

C.5.2.2.2 GCCS

- CJCSI 3155.01 Global Command and Control System – Joint Operational Frame Work Policy, 10-May-2007.
- CJCSI 3151.01 Global Command and Control System Common Operational Picture Reporting Procedures, 19-Jan-2007.
- CJCSI 6731.01 Global Command and Control System Security Policy, 30-Aug-2006.
- U.S. Central Command Regulation 25 – 22 USCENTRAL COMMAND Global Command and Control System Program instruction.
- US CENTRAL COMMAND GCCS COP CONOPS
- DII Assets Distribution System (DADS)

C.5.2.2.3 End User Hardware Maintenance Support

- USCENTCOM Regulation 735-2 Automated Data Processing Equipment (ADPE) Inventory, Control, and disposition.

C.5.2.2.5 Wireless Support

- USCENTCOM Regulation 105-7 Voice Communication Services
- USCENTCOM Regulation 105-10 Communications Security (COMSEC) Monitoring

C.5.2.3.1 Visual Information Systems

- CCR 105-12 Video Teleconference Program

C.5.2.3.2 Security Cooperation Offices (SCO) Support

- DISAC 300-175-9, Global Information Grid (GIG) Operating-Maintenance Electrical Performance Standards, 24 July 2006.
- DISAC 310-70-1, DII Technical Control, 8 May 2006.
- DISAC 310-70-S1, DII Technical Control Test Descriptions, 8 May 2002.
- DISAC 310-55-1, Status Reporting, 8 May 2002.
- DISAC 310-55-9, Base Level Support for the Defense Information System Network (DISN), 12 July 2006.
- DISAC 310-65-1, Circuit and Trunk File Data Elements and Codes Manual of the Global Information Grid (GIG), 25 May 2006.
- DISAC 310-70-57, DII Quality Assurance Program, 21 April 2006.
- DISAC 310-130-1, Submission of Telecommunications Service Requests, 25 May 2006.
- Air Force Instruction 33-116, Long-Haul Telecommunications Management.
- AFMAN 23-110, Basic USAF Supply Manual.
- CCJ6-D Cable Labeling Standards SOP.
- CCR-25-75 Security Cooperation Organization (SCO) Information Systems Support, 20-Jan-2012.
- USCENTCOM Regulation 12-2, (Information Resource Management), 17-Jan-2007.
- USCENTCOM Regulation 25-206, (Network Operations), 21-Sep-2007.
- USCENTCOM Regulation 105-5, Defense Special Security Communications System Message Preparation, 30 December 1984.
- USCENTCOM Regulation 105-12, Video Teleconference Program, 17-Dec-2007.
- USCENTCOM Regulation 380-8 (Automated Information Systems (AIS) Security Program), 20-Aug-2001.
- USCENTCOM Regulation 525-31, Hurricane Preparedness Standing, 08-Nov-2007.
- CCR 310-3, Reproduction, Printing, Duplicating and Copying, 5-Feb-2010.
- USCENTCOM Regulation 37-13, (Internal Management Control Program), 01-Apr-1998.
- USCENTCOM Regulation 12-2, Security Assistance Policy, Administration and Management, 27-Jun-2002.
- USCENTCOM Regulation 25-101, USCENTCOM Mail Procedures, 26-Sep-2000.
- USCENTCOM Regulation 25-200, Information Systems Management, Policies and Responsibilities, 06-May-2002, w/change 1.
- USCENTCOM Regulation 25-207, U.S. Central Command Global Command And Control System Program Instruction, 15-Jan-2002.
- USCENTCOM Regulation 25-108, Information Management Records Management Policy.
- CCR 10-2 for maintaining existing programs.
- Chairman of the Joint Chiefs of Staff Manual CJCSIM 6231 series, Manual for Employing Joint Tactical Communications, 17-Nov-2000.
- DISA Circular 310-55-1, Status Reporting for DCS, 21-Jan-2000.
- DISA Circular 310-70-1, DII Technical Control, 25-Jun-1998.
- DISA Circular 310-70-57, DII Quality Assurance Program, 13-Apr-1998.

- DISA Circular 300-175-9, DII Operating-Maintenance Electrical Performance Standards, 08-Jun-1998.
- DoD Instruction (DoDI) 5200.40, 30-Dec-1997.
- DoDI 8510.1-M, 28-Nov-2007.
- NTISSP-8, National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Government, 13-Feb-1997.
- National Security Telecommunication and Information Systems Security (NSTISSI) 4007, Communications Security (COMSEC) Utility Program, Nov-2007.
- EKMS 1, Communications Security Material System 21A: CMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 and 3, 05-Oct-2004.
- All COMSEC directives in the following: AFI 33-215 (01-Jan-1998); and AFI 33-210.
- AFI 33-211 (01-Oct-1999), http://www.fas.org/irp/DoDdir/usaf/33-211.htm
- USCENTCOM Regulation 25-105, Forms Management Program, 02-Feb-2007.
- CCJ6 Network Operations Center Standard Operating Procedure #NOC 02-011, 22-Jul-2002.
- AFI 33-209

C.5.3.1 Level 0 Fault Monitoring, Identification, Resolution

- CENTCOM Regulation 25-1, Information Management Program, 19 Aug 2010
- CENTOM Regulation 25-206, Communications – Network Operations (NETOPS), 21 Sep 2007
- CENTCOM Regulation 10-2, USCENTCOM Organization and Functions, 28 Apr 2010
- CENTCOM Regulation 530-1, Operations Security, 27 Oct 2008
- DISAC 310-70-1, DII Technical Control, 25 Jan 1998
- DISAC 310-55-1, Status Reporting, 21 Jan 2000

C.5.3.2 Level 1 Current Operations

- CENTCOM Regulation 25-1, Information Management Program, 19 Aug 2010
- CENTOM Regulation 25-206, Communications – Network Operations (NETOPS), 21 Sep 2007
- CJCSI 3320.02E, Chairman of the Joint Chiefs of Staff Instruction, Joint Spectrum Interference Resolution (JSIR), 15 Oct 2010
- CJCSM 3320.02C, Chairman of the Joint Chiefs of Staff Manual, Joint Spectrum Interference Resolution (JSIR) Procedures, 28 Jan 2011
- CJCSM 6231.01D, Manual for Employing Joint Tactical Communications, 15 Jan 2010
- CENTCOM Regulation 10-2, USCENTCOM Organization and Functions, 28 Apr 2010
- CENTCOM Regulation 530-1, Operations Security, 27 Oct 2008
- DISAC 310-70-1, DII Technical Control, 25 Jan 1998
- DISAC 310-55-1, Status Reporting, 21 Jan 2000

C.5.3.3 Information Assurance – CND

- CENTCOM Regulation 25-1, Information Management Program, 19 Aug 2010

- CENTOM Regulation 25-206, Communications – Network Operations (NETOPS), 21 Sep 2007
- CENTCOM Regulation 10-2, USCENTCOM Organization and Functions, 28 Apr 2010
- CENTCOM Regulation 530-1, Operations Security, 27 Oct 2008
- CENTCOM Regulation 380-14, Security Classification Guide 0110, 26 Feb 2010

C.5.4 Engineering Support

- DoD Directive 5230.9, Clearance of DoD Information as Public Release, 21-Nov-2003.
- DoD Instruction 5230.29, Security and Policy Review of DoD Information for Public Release, 06-Aug-1999.
- DoD Directive 5400.11, DoD Privacy Program, 08-May-2007.
- DoD Directive 5400.11R, DoD Privacy Program, 14-May-2007.
- DoD Directive 5210.50, Unauthorized Disclosure of Classified Information to the Public, 22-Jul-2005.
- R141553Z, Website OPSEC Secretary of Defense Message, Jan-2003, http://www.DoD.mil/webmasters/policy/rumsfeld_memo_to_DoD_webmasters.html.
- Web Site Administration Policies and Procedures, 11-Jan-2002, http://www.defenselink.mil/webmasters/policy/DoD_web_policy_12071998_with_amendments_and_corrections.html.
- DoD Directive (DoDD) 5144.1, Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer (ASD(NII)/DoD CIO), 02-May-2005, http://www.dtic.mil/whs/directives/corres/pdf/514401p.pdf.
- DoDD 8320.02, Data Sharing in a Net-Centric Department of Defense, 04-23-2007, http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf.
- DoD Instruction (DoDI) 8115.02, Information Technology Portfolio Management Implementation, 30-Oct-2006, http://west.dtic.mil/whs/directives/corres/pdf/811502_103006/811502p.pdf.
- Architecture Development Method (ADM), "TOGAF Enterprise Edition," v8.1, http://www.opengroup.org/architecture/togaf8-doc/arch/, 2004.
- Chairman, Joint Chiefs of Staff, Instruction, CJCSI 3170.01E, Joint Capabilities Integration and Development System (JCIDS), 11 May 2005, http://hqinet001.hqmc.usmc.mil/PP&O/PLN/Files/JSPS/Dev%20Strategy/CJCSI%203170-01%20JCIDS.pdf.
- CJCSI 6212.01C, Interoperability and Supportability of Information Technology and National Security Systems, 8 March 2006
- CJCSM 3170.01B, Operation of the Joint Capabilities Integration and Development System (JCIDS), 11 May 2005, https://acc.dau.mil/CommunityBrowser.aspx?id=19936.
- AFI 33-401, IMPLEMENTING AIR FORCE ARCHITECTURES, 14-Mar-2007, http://www.e-publishing.af.mil/shared/media/epubs/AFI33-401.pdf.
- Department of Defense Architecture Framework Version 1.5, Volume I: Definitions and Guidelines, 23 April 2007, http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_I.pdf.

- Department of Defense Architecture Framework Version 1.5, Volume II: Product Descriptions, 23 April 2007, http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_II.pdf.
- Department of Defense Architecture Framework Version 1.5, Volume III: Architecture Data Descriptions, 23 April 2007, http://www.defenselink.mil/cio-nii/docs/DoDAF_Volume_III.pdf.
- Department of Defense Joint Publication, JP 1-02, "Dictionary of Military and Associated Terms," Joint Publication 1-02, August 2002, http://www.fas.org/irp/doddir/dod/jp1_02.pdf.
- DoDD 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 5 May 2005, http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf.
- DoDD 5000.1, The Defense Acquisition System, May 12, 2003, http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf.
- DoDD 8000.1, Management of DoD Information Resources and Information Technology, 27 February 2002; Administrative Reissuance, 20 March 2002, http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf.
- DODD 8100.01, Global Information Grid Overarching Policy, 19 September 2002, http://www.dtic.mil/whs/directives/corres/pdf/810001p.pdf.
- DODD 8115.1, Information Technology Portfolio Management, 10 October 2005, http://www.dtic.mil/whs/directives/corres/pdf/811501p.pdf.
- DoD 8320.02-G, Guidance for Implementing Net-Centric Data Sharing, ASD(NII) CIO, 12 April 2006, http://www.dtic.mil/whs/directives/corres/pdf/832002g.pdf.
- DODI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004, http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf.
- DODI 5000.2, Operation of the Defense Acquisition System, 12 May, 2003, http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf.
- "Federal Enterprise Architecture Program EA Assessment Framework 2.1,", December 2006, http://www.whitehouse.gov/omb/egov/documents/OMB_EA_Assessment_Framework_v21_Final.pdf.
- "Federal Enterprise Architecture Data Reference Model", v2.0, 17 November 2005, http://www.whitehouse.gov/omb/egov/documents/fea-drm1.PDF.
- Integration Definition for Function Modeling (IDEF0), Federal Information Processing Standards (FIPS) Publication 183, 21 December 1993, http://www.idef.com/pdf/idef0.pdf.
- Integration Definition for Data Modeling (IDEF1X), Federal Information Processing Standards (FIPS) Publication 184, 21 December 1993, http://www.idef.com/pdf/Idef1x.pdf.
- Information Integration For Concurrent Engineering (IICE) IDEF3, Process Description Capture Method Report, KBSI-IICE-90-STR-01-0592-02, Knowledge Based Systems, Incorporated, 1995, http://www.idef.com/pdf/Idef3_fn.pdf .
- "Recommended Practice for Architectural Description of Software-Intensive Systems," IEEE Std 1471, 2000, http://www.ieee.org.

- Institute of Electrical and Electronics Engineers, IEEE STD 610.12, Standard Glossary of Software Engineering Terminology, http://standards.ieee.org/cgi-bin/status?610.12-1990.
- Allied Data Publication 34, NATO C3 Technical Architecture, Volume 2: Architectural Descriptions and Models, v4.0, 7 March 2003, pp. 35-38, 194.7.80.153/website/book.asp?menuid=15&.../NC3TA-Vol2-v7-internet.pdf.
- "DoD Net-Centric Data Strategy", Memorandum, 9 May 2003, http://www.defenselink.mil/nii/org/cio/doc/Net-Centric-Data-Strategy-2003-05-092.pdf.
- "Memorandum: Global Information Grid Enterprise Services (GIG ES) - Net-Centric Environment," OASD(NII), July 2004, http://www.defenselink.mil/nii/doc/docArchive.html#NII.
- Organization for the Advancement of Structured Information Standards (OASIS), "Reference Model for Service Oriented Architecture 1.0", OASIS Standard, 12 October 2006, http://www.oasis-open.org/specs/index.php#soa-rmv1.0.
- The Open Group Architecture Framework (TOGAF), v8.1, 2004, http://www.opengroup.org/architecture/togaf/.
- CCR 25-208.
- CCR 25-209.
- Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6231, Manual for Joint Tactical Communications.
- CENTCOM Regulation (CCR), 25-200, C1 (Information Systems Management, Policies and Responsibilities), 06-May-2002.
- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 8410, Warfighting Mission Area Information Technology Portfolio Management and Net-Centric Data Sharing, 22-Jun-2007.
- CENTCOM Regulation 25-206, Network Operations (NETOPS), 21-Sep-2007.
- CENTCOM Regulation 25-200, Information Resource Management, 25-Jan-2008.
- CENTCOM Instruction 5-1, Program/Project Management
- Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6215, Policy for Department of Defense Voice Networks with Real Time Services, 09-Nov-2007.
- CENTCOM Regulation 10-2, USCENTCOM Organization and Functions, 07-Feb-2007.
- CENTCOM Regulation 530-1, Operations Security, 08-Feb-2005.
- CJCSI 3320.03B, JCEOI, 16-Mar-2011.
- DoDD 3222.3, DoD E3 Compatibility Program, 08-Sep-2004.
- DoDD 3222.4, EW and Command Control Warfare Countermeasures, 28-Jan-1994.
- DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the DoD GiG, 14-Apr-2004.
- DoDI 4630.8, Procedures for Interoperability and Supportability for Information Technology and National Security Systems, 30-June-2004.
- Allied Communications Publication (ACP) 131(e) Communications Instructions Operating Signals, Mar-1997.
- ACP 190(C), Guide to Spectrum Management in Military Operations, Sept-2007.
- ACP 194, Policies for the Coordination of Military RF Allocations and Assignments between Cooperating Nations, Apr-2005.
- FM 3-04.15, Multi-Service TTP for the Tactical Employment of UAS, Aug-2006.

- FM 6-02.72, Multi-Service Communications Procedures for Tactical Radios in a Joint Environment.
- FM 6-02.74, Multi-Service TTP for HD-ALE Radios.
- FM 6-02.771, Multi-Service TTP for Have Quick Radios.
- CCR 25-206.
- CCR 10-12.
- Air Force Instruction (AFI) 33-201v2, Communications Security Requirements, 26-April-2005.
- NSTISSP-11, National Information Assurance Acquisition Policy, Jul-2003, http://www.cnss.gov/Assets/pdf/nstissp_11_fs.pdf.
- NSTISSP-101, National Policy on Secure Voice Communications, 14-Sep-01, http://www.cnss.gov/Assets/pdf/nstissp_101.pdf.
- CJCSI 6232.01D, Link 16 Spectrum Deconfliction, 20-Nov-2007, http://www.dtic.mil/doctrine/jel/cjcsd/cjcsi/6232_01b.pdf.
- NTIA Manual, http://www.ntia.doc.gov/osmhome/redbook/redbook.html.
- DoD 8570.01 – Information Assurance Training, Certification, and Workforce Management, 15-Aug-2004, http://www.dtic.mil/whs/directives/corres/pdf/857001p.pdf.
- USCENTCOM NETOPS CONOPS, Joint Concept of Operations for US Central Command Theater Information Grid NetOps, 30-Oct-2006.
- Joint Publication 6-1, Joint Communications System, 20-Mar-2006
- CJCSI 6251.01C, NARROWBAND SATELLITE COMMUNICATIONS TIME DIVISION MULTIPLE ACCESS REQUIREMENTS, 15-Aug-2009
- MCEB Pub 7.
- FSCS-217-98-00-1, Joint UHF DAMA Address Assignment and Distribution Guide.
- JSC-HDBK-05-001, Joint Spectrum Management Handbook, Oct-2005.
- CCR 525.18, Military Operations Electronic Warfare. *Secret Clearance Required*
- USCENTCOM Regulation 12-2, (Information Resource Management), 17-Jan-2007.
- USCENTCOM Regulation 25-206, (Network Operations), 21-Sep-2007.
- USCENTCOM Regulation 105-5, Defense Special Security Communications System Message Preparation, 30 December 1984.
- USCENTCOM Regulation 105-12, Video Teleconference Program, 17-Dec-2007.
- USCENTCOM Regulation 380-8 (Automated Information Systems (AIS) Security Program), 20-Aug-2001.
- USCENTCOM Regulation 525-31, Hurricane Preparedness Standing, 08-Nov-2007.
- CCR 310-3, Reproduction, Printing, Duplicating and Copying, 28-Sep-2006.
- CINCCENT Theater Engagement Plan Strategic Concept FY02-04, USCINCCENT Plan 1250-01, 01-Apr-2001.
- President's 19-Nov-1999 letter, Cooperative Defense Initiative (CDI).
- USCENTCOM Coalition Interoperability Plan-27 Feb 2001.
- CCJ2 Combined Communications Enterprise Requirements, Apr-2001.
- USCENTCOM Regulation 37-13, (Internal Management Control Program), 01-Apr-1998.
- USCENTCOM Regulation 12-2, Security Assistance Policy, Administration and Management, 27-Jun-2002.

- USCENTCOM Regulation 25-101, USCENTCOM Mail Procedures, 26-Sep-2000.
- USCENTCOM Regulation 25-105, Forms Management Program, 02-Feb-2007.
- USCENTCOM Regulation 25-200, Information Systems Management, Policies and Responsibilities, 06-May-2002, w/change 1.
- USCENTCOM Regulation 25-207, U.S. Central Command Global Command And Control System Program Instruction, 15-Jan-2002.
- USCENTCOM Regulation 25-108, Information Management Records Management Policy.
- CCJ6 Network Operations Center Standard Operating Procedure #NOC 02-011, 22-Jul-2002.
- CCR 10-2 for maintaining existing programs.
- Chairman of the Joint Chiefs of Staff Manual CJCSIM 6231 series, Manual for Employing Joint Tactical Communications, 17-Nov-2000.
- DISA Circular 310-55-1, Status Reporting for DCS, 21-Jan-2000.
- DISA Circular 310-70-1, DII Technical Control, 25-Jun-1998.
- DISA Circular 310-70-57, DII Quality Assurance Program, 13-Apr-1998.
- DISA Circular 300-175-9, DII Operating-Maintenance Electrical Performance Standards, 08-Jun-1998.
- DoD Instruction (DoDI) 5200.40, 30-Dec-1997.
- DoDI 8510.1-M, 28-Nov-2007.
- NTISSP-8, National Policy Governing the Release of Information Systems Security (INFOSEC) Products or Associated INFOSEC Information to Foreign Government, 13-Feb-1997.
- National Security Telecommunication and Information Systems Security (NSTISSI) 4007, Communications Security (COMSEC) Utility Program, Nov-2007.
- EKMS 1, Communications Security Material System 21A: CMS Policy and Procedures for Navy Electronic Key Management System Tiers 2 and 3, 05-Oct-2004.
- All COMSEC directives in the following: AFI 33-211 (01-Oct-1999), http://www.fas.org/irp/DoDdir/usaf/33-211.htm; AFI 33-209, AFI 33-215 (01-Jan-1998); and AFI 33-210.

C.5.6 Programs and Architectures Support

- DoD Directive (DoDD) 5144.1, Assistant Secretary of Defense for Networks and Information Integration / DoD Chief Information Officer (ASD(NII)/DoD CIO), 02-May-2005, http://www.dtic.mil/whs/directives/corres/pdf/514401p.pdf.
- DoDD 8320.02, Data Sharing in a Net-Centric Department of Defense, 04-23-2007, http://www.dtic.mil/whs/directives/corres/pdf/832002p.pdf.
- DoD Instruction (DoDI) 8115.02, Information Technology Portfolio Management Implementation, 30-Oct-2006, http://www.dtic.mil/whs/directives/corres/pdf/811502p.pdf.
- Architecture Development Method (ADM), “TOGAF Enterprise Edition,” v8.1.1, http://www.opengroup.org/architecture/togaf8-doc/arch/, August 2006.

- Chairman, Joint Chiefs of Staff, Instruction, CJCSI 3170.01E, Joint Capabilities Integration and Development System (JCIDS), 1 March 2006, http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf.
- CJCSI 6212.01E, Interoperability and Supportability of Information Technology and National Security Systems, 15 December 2008, http://www.dtic.mil/cjcs_directives/cdata/unlimit/6212_01.pdf.
- CJCSI 3170.01G, Joint Capabilities Integration and Development System (JCIDS), 10 January 2012, http://www.dtic.mil/cjcs_directives/cdata/unlimit/3170_01.pdf.
- AFI 33-401, AIR FORCE ARCHITECTURES, 17 May 2011, http://www.af.mil/shared/media/epubs/AFI33-401.pdf.
- Department of Defense Architecture Framework Version 2.02, August 2010, http://dodcio.defense.gov/sites/dodaf20/products/DoDAF_v2-02_web.pdf.
- Department of Defense Joint Publication, JP 1-02, "Dictionary of Military and Associated Terms," Joint Publication 1-02, 8 November 2010, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf.
- DoDD 4630.5, Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 5 May 2004, http://www.dtic.mil/whs/directives/corres/pdf/463005p.pdf.
- DoDD 5000.01, The Defense Acquisition System, May 12, 2003, http://www.dtic.mil/whs/directives/corres/pdf/500001p.pdf
- DoDD 8000.1, Management of DoD Information Enterprise, 10 February 2009 http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf.
- DoD 8320.02-G, Guidance for Implementing Net-Centric Data Sharing, ASD(NII) CIO, 12 April 2006, http://www.dtic.mil/whs/directives/corres/pdf/832002g.pdf.
- DODI 4630.8, Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS), 30 June 2004, http://www.dtic.mil/whs/directives/corres/pdf/463008p.pdf.
- DODI 5000.2, Operation of the Defense Acquisition System, 8 December 2008 , http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf.
- "Federal Enterprise Architecture Program EA Assessment Framework 2.2,", October 2007, http://www.cioindex.com/nm/articlefiles/50197-OMB_EA_Assessment_Framework_v22_Final.pdf
- "Federal Enterprise Architecture Data Reference Model", v2.0, 17 November 2005, http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/DRM_2_0_Final.pdf
- Integration Definition for Function Modeling (IDEF0), Federal Information Processing Standards (FIPS) Publication 183, 21 December 1993, http://www.idef.com/pdf/idef0.pdf.
- Integration Definition for Data Modeling (IDEF1X), Federal Information Processing Standards (FIPS) Publication 184, 21 December 1993, http://www.idef.com/pdf/Idef1x.pdf.
- Information Integration For Concurrent Engineering (IICE) IDEF3, Process Description Capture Method Report, KBSI-IICE-90-STR-01-0592-02, Knowledge Based Systems, Incorporated, 1995, http://www.idef.com/pdf/Idef3_fn.pdf .

- "Recommended Practice for Architectural Description of Software-Intensive Systems," IEEE Std 1471, 2000, http://www.ieee.org.
- Institute of Electrical and Electronics Engineers, IEEE STD 610.12, Standard Glossary of Software Engineering Terminology.
- Allied Data Publication 34, NATO C3 Technical Architecture, Volume 2: Architectural Descriptions and Models, v4.0, 7 March 2003, pp. 35-38, 194.7.80.153/website/book.asp?menuid=15&.../NC3TA-Vol2-v7-internet.pdf.
- "DoD Net-Centric Data Strategy", Memorandum, 9 May 2003, http://dodcio.defense.gov/docs/Net-Centric-Data-Strategy-2003-05-092.pdf
- Organization for the Advancement of Structured Information Standards (OASIS), "Reference Model for Service Oriented Architecture 1.0", OASIS Standard, 12 October 2006, http://www.oasis-open.org/specs/index.php#soa-rmv1.0.
- The Open Group Architecture Framework (TOGAF), v8.1, 2004, http://www.opengroup.org/architecture/togaf/
- CJCSI 6510.06B, COMMUNICATIONS SECURITY RELEASES TO FOREIGN NATIONS, 31 Mar 11
- CCR 10-5, USCENTCOM Command and Control Interoperability Element, 14 April 11

C.5.7.1 Records Management

- CCR 25-108, Information Management Records Management Policy.
- Department of Defense Directive, 5015.2 Records Management Program, 06-Mar-2000.
- Chairman of the Joint Chiefs of Staff Manual (CJCSM), 5760.01A Vol. I, Joint Staff and Combatant Command Records Management Manual: Procedures, 30-Apr-2007.
- CJCSM 5760.01 Vol II, Joint Staff and Combatant Command Records Management Manual: Disposition Schedule, 10-Mar-2003.
- DoD 5015.02-STD, Electronic Records Management Software Applications Design Criteria Standard, 25-Apr-2007.
- DoD 5400.11R, Department of Defense Privacy Act Program, 14-May-2007.

C.5.7.2 Asset Management Support

- AF Manual 23-110, Vol 2, Part 2, Chp 2, Organization and Responsibilities
- AF Manual 23-220, Reports of Survey for Air Force Property.
- AF Manual 23-110, Vol 2, Chp 22, Equipment Management.
- DRMS 4105.2, Procedures for Preparation of Requests for Supplies and Services.
- US Central Command Regulation 735-2 Automated Data Processing Equipment (ADPE) Inventory, Control, and Disposition.

jean.mulligan-wasser@gsa.gov

Attachment O
Deliverable Acceptance-Rejection Report

DELIVERABLE ACCEPTANCE/REJECTION FORM

Dear (insert name of TPOC)

Please review the deliverable identified below, sign and date, and provide any comments either in the space provided or on an attached form. Comments are due by **XX/XX/20XX**.

DELIVERABLE NAME:
AGENCY NAME:
PROJECT NAME:
FEDSIM TASK ORDER/CONTRACT NUMBER:
FEDSIM PROJECT NUMBER:
DELIVERABLE DUE DATE:

I have reviewed the aforementioned document and have:
☐ Accepted it without comments
☐ Accepted it with comments
☐ Rejected it with comments

COMMENTS:

_____ _____
(name) (date)
(title)

Attachment P
Background and Sizing Information

Proposed C4 Enterprise Task Order Request (TOR)
USCENTCOM Background Portion

USCENTCOM

USCENTCOM is one of nine Department of Defense (DoD) unified commands. The Command activated in January 1983 as the successor to the Rapid Deployment Joint Task Force. USCENTCOM, with its headquarters (HQ) located at MacDill Air Force Base (AFB), Florida, is the unified command responsible for U.S. security interests in the 27 nations of the Central Region that stretch from the Horn of Africa through the Arabian Gulf region, into Central Asia. This area of responsibility (AOR) is located 7,000 air miles from America's East Coast.

Mission: With national and international partners, United States Central Command promotes cooperation among nations, responds to crises, and deters or defeats state and non-state aggression, and supports development and, when necessary, reconstruction in order to establish the conditions for regional security, stability, and prosperity.

Officially, the HQ staff totals over 1,200 personnel and includes members of each military Service. During periods of heightened operations, the HQ increases, as required, with Service augmenters and Reservists. Each of the Services also provides USCENTCOM with Component Commands, which, along with our Joint Special Operations Component, make up USCENTCOM's primary warfighting and security cooperation organizations. The Component Commands and their primary HQ locations are:

USARCENT, U.S. Army Forces Central Command, Fort McPherson, Georgia
USMARCENT, U.S. Marine Forces Central Command, Camp Pendleton, California / MacDill AFB, Florida
USNAVCENT, U.S. Naval Forces Central Command, Manama, Bahrain
USAFCENT, U.S. Air Forces Central Command, Shaw Air Force Base, South Carolina
USCENTCOM Forward Headquarters (CFH), Al Udeid Air Base, Qatar
HQ Camp Arifjan, Kuwait
SOCCENT, Special Operations Command, Central, MacDill Air Force Base, Florida

USARCENT: USARCENT is the Army Component HQ of USCENTCOM. When so designated by the Commander, USCENTCOM (CDRUSCENTCOM), Commander, USARCENT (COMUSARCENT) functions as a Combined Force Land Component Commander (CFLCC) or Joint Force Land Component Commander (JFLCC). COMUSARCENT develops and coordinates requirements and plans for employment of U.S. Army forces and, when so directed, Joint/multinational land forces. USARCENT provides command and control (C2) of assigned and attached U.S. Army and designated Joint/multinational land forces operating within the USCENTCOM AOR.

USARCENT prepares continuously for rapid response to a major theater war and the diversity of operations other than war that characterize the Central Region. USARCENT provides strategic combat forces for power projection and sustained land combat. In addition to its combat capabilities, USARCENT provides essential logistics, communications, engineering, and medical support to all deployed Services. Its posture reflects the United States Army's emergence as a power projection force and acceptance of diverse and demanding missions.

Despite having few permanently stationed forces in the Central Region, USARCENT's ability to respond across the spectrum of military operations has greatly improved through prepositioning enhancements and the establishment of deployed HQ sites in Kuwait and Qatar.

The Kuwait prepositioning site continues to set the standard for maintaining and distributing a brigade's combat equipment. Brigade combat teams have successfully deployed to Kuwait. Soldiers, flown to Kuwait from their home bases in the United States, can draw their equipment and move to pre-assigned fighting sites within hours of landing. These deployments, and the realistic training conducted by the brigades while in Kuwait, validate the Command's innovative concepts for projecting power to the Region.

USMARCENT: Commander, USMARCENT (COMUSMARCENT) provides Marine expeditionary forces capable of conducting a wide-range of operations, offering the Command a responsive and unique set of capabilities. Marines embarked aboard U.S. Navy amphibious ships deploy regularly to the Region organized as Marine Air Ground Task Forces (MAGTF). As Marine Expeditionary Units Special Operations Capable (MEU SOC), these forces provide a potent mix of capabilities that can project expeditionary combat power rapidly to any location in the Region. While afloat in the Central Region, they serve as a visible deterrent force, train continuously, and participate in a wide-range of engagement activities. In addition to providing MAGTFs deployed aboard U.S. Navy ships, USMARCENT has the proven capability to deploy MAGTFs to the Central Region by air or fast sea transport. These Marines can marry-up with prepositioned equipment, providing USCENTCOM with a rapid response capability across the full spectrum of military operations.

USNAVCENT: Commander, USNAVCENT (COMUSNAVCENT) exercises command and control (C2) over all naval operations throughout the AOR from a HQ located in Manama, Bahrain. When so designated by CDRUSCENTCOM, COMUSNAVCENT functions as a Combined Force Maritime Component Commander (CFMCC) or a Joint Force Maritime Component Commander (JFMCC). CFMCC's mission is to deal with and defeat transnational threats to include international terrorism. Specifically, CFMCC will deter terrorists from using the maritime environment and disrupting terrorist attack planning. CFMCC accomplishes this mission by conducting maritime security operations (MSO) throughout the theater, in synchronization with operations conducted by air and land component commanders, and in coordination with regional nations. CFMCC complements the counter-terrorism activities of regional Navies and Coast Guards through exercises, training and coordinated operations. The global coalition against terrorism includes members of CFMCC and the nations in the region. We share a common purpose: To preserve the free and secure use of the world's oceans

by legitimate mariners, and prevent terrorists from attempting to use the world's oceans as a venue for attack or as a medium to transport personnel or material.

USNAVCENT's location in the Central Region is an integral part of USCENTCOM's ability to execute an AOR strategy successfully. From MSO to major exercises, USNAVCENT plays a major role in maintaining stability and deterring aggression in the Region. The vast majority of USNAVCENT's operating forces rotationally deploy to the region from either the Pacific Fleet or the Atlantic Fleet. These forces normally consist of an Aircraft Carrier Strike Group (CSG), an Expeditionary Strike Group (ESG) with an embarked Marine Expeditionary Unit, surface combatants, submarines, maritime patrol and reconnaissance aircraft, and logistics ships.

In peacetime, USNAVCENT forces provide a forward presence capability that land-based forces cannot duplicate. By remaining in international waters, these forces are able to operate without infringing on national sovereignty or requiring overflight or shorebasing permission. This greatly enhances versatility and responsiveness by dramatically reducing reaction time in a crisis.

Should deterrence fail, forces of USNAVCENT are poised to establish and maintain maritime superiority on, over, and under the seas, as well as on the littoral land areas of the region. This unmatched capacity for dominating the multi-dimensional battlespace plays a key role in the CDRUSCENTCOM's ability to execute a comprehensive campaign plan successfully.

CFH: The forward headquarters of United States Central Command is located at Al Udeid Air Base, a military base located west of Doha, Qatar and the Abu Nahlah Airport. The primary purpose of CFH is to exercise the USCENTCOM staff's ability to seamlessly transition command and control of operations from its headquarters in Tampa to the new headquarters in Qatar in the event of a crisis in the USCENTCOM area of responsibility or a natural disaster in Florida. There are currently about 900 personnel stationed there. It also hosts the No. 83 Expeditionary Air Group RAF and the 379th Air Expeditionary Wing of the USAF. It houses foreign coalition personnel and assets.

USAFCENT: Plans for, and projects, decisive air and space power for USCENTCOM in the Central Region. When directed by CDRUSCENTCOM, the Commander, U.S. Central Air Forces (COMUSAFCENT) functions as a Combined Force Air Component Commander (CFACC) or a Joint Force Air Component Commander (JFACC). USAFCENT missions range from providing humanitarian airlift to integration of multinational forces into coherent air operations in support of full-scale warfare. With tactical aircraft, strategic reconnaissance, and intelligence collection capabilities, the USCENTCOM Air Component orchestrates multinational air operations in support of Operation ENDURING FREEDOM (OEF) and Operation IRAQI FREEDOM (OIF). By positioning within the theater with lethal anti-armor capabilities, USAFCENT forces create credible deterrence. If deterrence fails, USAFCENT is postured to gain and maintain air superiority as the first step towards achieving mission success across the operations continuum, including full-scale operations. USAFCENT consists of HQ Ninth Air Force, plus Air Force units supporting USCENTCOM mission requirements.

USAFCENT exercises procedures to integrate joint and combined forces, beginning with a common operations order and encompassing common language and operating procedures. For example, when an Airborne Warning and Control System (AWACS) aircraft commits a four-ship formation of fighters to intercept, identify, and destroy hostile airborne targets, it uses the same code words whether the fighters bear U.S., Saudi Arabia, Kuwaiti, or Egyptian markings. Integration ensures the full range of capabilities vested in airpower applied in simultaneous and continuous operations.

USAFCENT enhanced its global power projection capability through infrastructure improvements, propositioning of equipment and supplies, and the development of rapidly deployable Air and Space Expeditionary Forces (AEF). An AEF deployment supports exercises and operations and demonstrates USAFCENT's global reach.

HQ CAMP ARIFJAN: USTRANSCOM AND USCENTCOM recently organized a new strategic-level staff called the USCENTCOM Deployment Distribution Operations Center (CDDOC) and colocated it with the land-component headquarters at Camp Arifjan. The CDDOC synchronizes & optimizes strategic & theater multi-modal resources to maximize distribution, force movement, and sustainment logistics in support of USCENTCOM Theater. Overall, Camp Arifjan is an Army installation located in the State of Kuwait and used as a forward logistics base, Aviation Classification and Repair Activity Depot (Task Force AVCRAD) for the entire Southwest Asian Theater (through Patton Army Air Field), helicopter ground support base, and as a motor pool for armored and unarmored vehicles. The camp also accommodates elements of the U.S. Air Force, Navy, Marine Corps and Coast Guard. Military personnel from the United Kingdom, Australia, Romania and Poland are also forward deployed there. Camp Arifjan is located south of Kuwait City, and west of the Shuaiba Port (Military Sea Port of Debarkation/Embarkation, or SPOD) and Kuwait Naval Base (KNB).

SOCCENT: SOCCENT is a sub-unified command organized under CDRUSCENTCOM to implement the Command's AOR Strategy through special operations initiatives and programs that improve host-nation capabilities. SOCCENT's culturally sensitive forces provide a direct and unobtrusive link to our coalition counterparts and work to formalize procedures, agreements, and doctrine for combined warfare.

Although HQ SOCCENT is in Tampa, the command maintains a forward presence through the HQ SOCCENT Forward and C2 elements in Iraq and Afghanistan. Additional forces support Command programs to improve host nation capabilities. Command programs include a rigorous Joint Chiefs of Staff (JCS) exercise schedule, robust Joint Combined Exchange Training (JCET), and Small Unit Exchange (SUE) programs. SOCCENT's involvement in exercises contributes to increased trust and influence within the Region by providing valuable military-to-military contact and training at the unit level.

USCENTCOM AOR: The USCENTCOM region spans 6.5 million square miles and 20 countries including Iraq, Afghanistan, Iran, Egypt, the countries of the Horn of Africa, Jordan, Syria, Lebanon, the countries of the Arabian Peninsula, Pakistan, and the Central Asian states as far north as Kazakhstan. It incorporates a nexus of vital transportation and trade routes, including the Red Sea, the Northern Indian Ocean, and the Arabian Gulf. It is home to the

strategic maritime choke points of the Suez Canal, the Bab el Mandeb, and the Strait of Hormuz. It encompasses the world's most energy-rich region – the Arabian Gulf alone accounts for 57% of the world's crude oil reserves, 28% of the world's oil production, and 41% of the world's natural gas reserves.

The more than 650 million people who live in the region make up at least 18 major ethnic groups of many nationalities and cultures. While predominantly Muslim, the region is home to adherents of all of the world's major religions. Human civilization had its birth in this region, with many cities dating back thousands of years. The diverse peoples of the region take understandable pride in their rich culture and history.

Economic, social, and political conditions vary greatly from one nation to another, with per capita incomes ranging from $200 to nearly $40,000. Many countries in the region suffer from pervasive corruption, low economic growth, and high unemployment that is likely to persist given the high proportions of young men and women relative to overall populations. Some governments remain hard pressed to meet popular demands for economic opportunity, more social services, and increased political participation. But in the past year, the region has also witnessed dramatic, if incremental, progress in some of these areas. We have ousted the Taliban and Saddam Hussein, liberated fifty million people from tyranny and created an environment where democracy can emerge. Watershed elections in Iraq and Afghanistan have the potential to spur regional reform. We have enabled key partners to attack al Qaida, improve border security, and take an aggressive stand against extremists. Persistent effort across many fronts is necessary to ensure these accomplishments take hold and are not lost. A synchronized approach applying all four elements of national power (Diplomatic, Information, Military and Economic) is necessary for continued success.

Many in the region have renewed hopes for greater prosperity and political opportunity. At the same time, the many complex insurgencies and extremist and terrorist groups in the region feed on the fear of rapid change in a dynamic world that is increasingly interconnected. The challenge for the people in the region is to manage change without resorting to organized violence and at a pace that promotes rather than erodes stability. The challenge for the United States is two-fold: help people manage change without turning to the dark ideology of extremism and continue working to defeat the existing extremist network.

Defeating extremism will require significant effort among our allies and partners throughout the world. Internationalizing the effort will strengthen regional stability and garner support for the Long War. The U.S. cannot meet these challenges alone. Negotiating the transitional period ahead requires unity of effort from a capable and enabled coalition of partner nations. As USCENTCOM goes forward, USCENTCOM we must assist our partners in improving their capabilities to maintain security and fight terrorism and extremism both within their own borders and regionally.

Irregular Threats

The Al Qaida Network. The Al Qaida Network is the greatest current threat to international peace and stability, and the USCENTCOM AOR is its physical, ideological, and cultural locus.

This network of terrorist cells operates as a global web of leaders, fighters, weapons makers, financiers, facilitators, educators and trainers, and recruiters. Collectively, within the minds of its adherents, the network functions as a "Virtual Caliphate" guided by an extremist ideology that is central to its continued existence. As we continue to push into its geographic sanctuaries, the network will further disperse and metastasize, adapting in order to survive. However, in order to expand its operations on the regional and global levels, the network must find additional physical footholds throughout the AOR for use as bases of recruiting, financing, and propagating its ideology. This expansion into physical footholds advances the eventual establishment of a pan-Islamic, "Physical Caliphate," firmly anchored in the Middle East, and whose power and influence extends to Europe, Asia, and the Americas.

National-level Insurgencies**.** The threat of national-level insurgencies presents a challenge in many states throughout the region, and shapes the way they configure their military and security forces, lead their people, and deal with other states in the region. In some cases, these insurgent movements will align themselves with the Al Qaida network, calling upon Al Qaida for guidance, support, and legitimacy as they seek to supplant legitimate governments and replace them with theocratic states -- all steps in the realization of Al Qaida's vision of the eventual establishment of the Physical Caliphate. In other cases, national-level insurgencies may be launched separate from Al Qaida's influence and will be based upon local concerns and geared toward more local objectives.

Other Terrorist Organizations**.** Finally, terrorist organizations with no association to Al Qaida's unique strain of Sunni-based extremism exist in large degree in the USCENTCOM AOR and are a pervasive threat to the stability of the region. Shi'a-based terrorist organizations have deep roots in several locations throughout the AOR, particularly in the Levant and Iraq. State sponsorship makes it possible for groups actively seeking to destabilize the region, to plan, gather resources, and operate. Although these groups have not demonstrated the will to attack U.S. interests directly since 2001, their potential to do so makes them a very real threat throughout the region.

Catastrophic Threats

The proliferation of Weapons of Mass Destruction (WMD) at both the state and non-state levels presents a significant continual challenge. The potential for wide-spread destruction, enormous loss of life, and the attendant psychological shock of a WMD attack make this one of the more difficult and consequential problem-sets in the USCENTCOM AOR.

Four states within the AOR have a declared WMD capability of some kind, and five additional countries in the region have ballistic missile programs. Iran has declared its intention to pursue advanced nuclear programs, and has undertaken a sustained effort to develop nuclear weapons. The potential for a strategic miscalculation between WMD-capable states, or of WMD-related materials falling into the hands of terrorists and non-state actors by either theft or sale, makes the proliferation of WMD the single greatest catastrophic threat in the region.

Al Qaida has repeatedly demonstrated its intent to acquire a WMD and to use it against U.S. interests. Preventing them from matching that intent with a viable capability is one of

USCENTCOM's highest priorities.

Disruptive Threats

The vulnerability created by the international economy's dependence on petroleum is manifested in the USCENTCOM AOR by the high density of oil and natural gas reserves, the large number of refining and processing facilities, and the vital sea lanes that carry petroleum products to the global marketplace. Terrorist organizations, intent on attacking the economic vitality of the U.S. and damaging the global economic system, are likely to attempt coordinated attacks against the region's petroleum infrastructure.

Conventional Threats

The direct consequences of conventional warfare involving the U.S., and the indirect consequences of state-on-state conflict have the potential to de-stabilize the region and limit USCENTCOM's freedom of action for the foreseeable future.

Iran presents the most significant conventional threat to U.S. interests in the USCENTCOM AOR. Iran's conventional military power is considerable. It continues to improve its ballistic missile capability and has steadily moved toward the development of nuclear weapons. Iran has gradually improved its naval forces, and has the capability to influence the free flow of oil and other goods through the Arabian Gulf and the Strait of Hormuz. Iranian ground and air defense forces, -- although defensive in nature, -- continue to be improved and modernized in an Iranian effort to increase its stature as a regional military power. Iran is also a significant state sponsor of terrorism, which provides a latent capability to be used for asymmetrical attacks against U.S. and Western interests, -- both inside and outside the AOR, -- in the event of conventional conflict.

Syria's role in regional instability presents an additional long-term challenge within the USCENTCOM AOR. Syria's conventional military forces present no viable offensive threat to its neighbors. However, Syria maintains a significant capacity to defend itself from attack, possesses a considerable ballistic missile capability, and its air force is one of the largest in the Middle East. Although Syria has withdrawn its ground forces from Lebanon, Syria will likely continue to exert influence over its former client state through less visible means. Lingering mistrust over Syria's role in Lebanon and its initial intransigence over supporting coalition efforts in Iraq will continue to present a conventional challenge within the region.

Environmental Challenges

The irregular, catastrophic, disruptive, and conventional threats in the USCENTCOM AOR all exist within a regional environment that is itself challenging and limits USCENTCOM's freedom of action across the range of military operations, from shaping to decisive operations engagements.

The Clash of Ideas within Islam. The rise of Al Qaida and its associated movements has laid bare an ideological struggle within Islam itself. This struggle pits the violent and reactionary fringe elements of Islam against the vast majority of the Muslim population throughout the AOR that finds the adversary's militancy and brutal tactics repugnant. Within the region, there is a

significant and well-meaning concern over Islam's ability to maintain its religious and cultural identity in the face of increasing secularization and Westernization -- two of the defining features of the modern world. But while a small element of the Muslim population at large has chosen to externalize that struggle through violence, terrorism, and advocating open warfare with non-Muslims, the majority of the Muslim population has rejected either the foundation of that ideology, or its violent manifestations, as contrary to the Islamic faith. This clash of ideas, already a major feature of the regional environment, will become even more prominent in the years to come as those who reject the enemy's militant Islamic ideology become more vocal and willing to take action against those who are advancing an agenda of hostility and bloodshed under the cloak of protecting the Islamic faith.

Ungoverned Areas. A large number of ungoverned spaces within the AOR provide adversaries the ability to train, operate, gather resources, and sustain operations free from governmental interference and, in some cases, with the active support of local leaders. The number and size of ungoverned areas in the region give the enemy the anonymity and relative freedom from detection they need, and the enemy will continue to seek out these ungoverned areas for further use and exploitation.

Internal State Instability. The stability of all nations in the AOR presents a key regional challenge. Al Qaida and its associated movements are actively seeking to undermine the stability of several states in the region in a deliberate attempt to expand their physical presence in the AOR and move toward the establishment of the Physical Caliphate. In doing so, they will focus their efforts on those states within the AOR who suffer from a combination of relatively weak or unpopular governments and populations seeking change. The enemy inflames popular discontent and positions itself as the rightful alternative to the government with promises to return the nation to an age of influence and Islamic purity. Having done that, the enemy is in a position to usurp the government. Forestalling this process of de-stabilization, and eventually supplanting these governments will present a key challenge in the years to come.

The Youth Bulge. Twenty-two of the twenty-seven countries in the AOR have at least forty percent of their populations between the ages of fifteen and twenty-nine, making those countries over twice as likely to experience outbreaks of civil violence. In nations where the youth population outpaces job growth, this large pool of young people -- facing a future of underemployment and marginal potential for a prosperous future -- will tend to be restive and prone to seek radical change. When combined with a political culture of repression and under-representation, Al Qaida and other terrorist organizations are provided a fertile environment in which to preach their message of hate, alienation, and perceived oppression, making a significant segment of that population predisposed to support the network as a fighter, facilitator, or passive supporter.

Israel and the Palestinian Issue. The Israeli-Palestinian issue remains a significant influence on the regional environment, and too often provides the lens through which US initiatives in the region are viewed. This issue has the potential to serve as a coalescing mechanism that Shi'a and Sunni extremists can use for common cause in their attempt to focus popular Arab and Muslim rage for use in propaganda, proselytizing, and terrorist recruitment. The Israeli-Palestinian issue

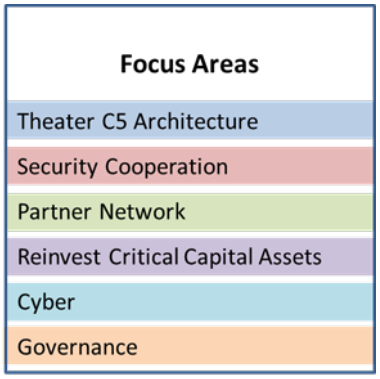
will remain a significant and challenging long-term feature of the USCENTCOM regional environment.

Other Regional Influences Other states bordering the USCENTCOM AOR influence the regional environment by advancing their national interests inside our region in ways that could potentially limit USCENTCOM's freedom of action in the years to come. Turkey has a large stake in the future of northern Iraq. India is the world's largest democracy, a declared nuclear state, and a burgeoning information-age powerhouse, placing it in a position to exert greater influence in Central Asia in the coming years. Russia attempts to hold sway over its former satellites in Central Asia, and remains a dominant player in the sub-region. China has begun the initial process of carving out a sphere of influence across its western border. Additionally, China's and India's ever-growing demand for fossil fuel has the potential to spark a higher level of regional competition that will be played out in the USCENTCOM AOR in the coming years.

USCENTCOM conducts operations to attack, disrupt and defeat terrorism, deter and defeat adversaries, deny access to WMD, ensure regional access, strengthen regional stability, build the self-reliance of partner nations' security forces, and protect the vital interests of the US within the area of responsibility.

C5 strategy

USCENTCOM Coalition, Command, Control, Communications and Computers (C5) Strategy: USCENTCOM is at the dawn of a major transition during the drawdown of two theater conflicts while continuing to prepare for future challenges with the recognition that we must make hard fiscal choices. This C5 strategy document aims to guide the USCENTCOM strategy and framework. The goal is to work with our mission partners to inform the Planning, Programming, Budgeting, and Execution System process to ensure our C5 transition meets the theater's future mission requirements during the near, mid, and long-term timeframes. This document outlines six focus areas and provides the basis of our engagement with the greater DoD C5 capability providers, supporting the Command's Theater Strategy, Campaign Plan, Security Cooperation and engagement efforts, and contingency plans.



Vision: The USCENTCOM C5 Enterprise is a balanced, robust, reliable, redundant, secure and rapidly restorable C5 capability that seamlessly interoperates regardless of location or environment to ensure operational flexibility fully enabling effective Command and Control.

Focus Areas: The guiding principles for the C5 Enterprise include Commander-centric, net-enabled capabilities focusing on effectiveness first. We must train how we fight before we enter the fight and align C5 Enterprise operational authorities with mission command authorities for greatest effect. This is accomplished by employing data/standards-driven architectures to maximize interoperability and information sharing while smartly balancing risk to the C5 Enterprise and operational imperative – integrating risk management with Enterprise decision making. The end result is a C5-ready Enterprise providing a "plug-and-play" environment suited for Partner, Combined, Coalition, and Multinational operations.

As USCENTCOM will work with internal and external partners to operationalize cyberspace through six equally relevant lines of transformation: Theater C5 Architecture-provide context and rules for accomplishing the "provide, operate and defend" missions; Security Cooperation-we must invest in partner-nation relationships through security cooperation via C5 resource sharing and Cyber defense preparation; Partner Network-a standing C5 mission platform available from the initial phase of operations where coalition partners are trained and familiar with the mission network; Reinvest Critical Capital Assets-Prepare for a fiscally constrained environment by getting ahead of the Services POM cycle and shaping Service provided capabilities to meet Command requirements; Cyber- our adversaries use of cyberspace as a warfighting domain does not necessarily respect international law; Governance- Utilize doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) to determine whether a given capability gap can be best addressed through a new defense acquisition program.

Theater C5 Architecture: The USCENTCOM theater C5 architecture remains in a constant state of flux due to changes in the strategic communications nodes, C5 Enterprise connectivity, and interoperability requirements. We must ensure robust, reliable, redundant, secure, survivable, restorable, and flexible warfighting command and control systems for the Command. USCENTCOM must have seamless system interoperability across the USCENTCOM theater -- the Arabian Peninsula, Levant, and Central and South Asia States sub-regions. Required data and information must flow quickly and efficiently. These capabilities must function on any platform, within any environment, supporting any coalition mission partner and interoperate with our existing joint, interagency, coalition, and other nation partner systems, all while assuring the proper information security levels.

Supporting our bandwidth optimization efforts yet continuing to support distributed operations in austere environments; tools, services and applications must be developed with latency tolerance and bandwidth efficiency in mind. Continuing to push data stores forward and relaying on smart pulls vice bulk pushes of data can significantly affect the overall capacity requirements and user experience. Pre-existing DISA facilities are well suited for this mission.

Security Cooperation: In line with DoD priorities for 21st century defense which emphasizes Gulf security, our C5 engagement strategy is to host recurring, multilateral engagements between

senior U.S. military communicators and central region partner nation military communicators to foster relationships, encourage international exchange and dialogue on regional telecommunications issues of common interest, and ultimately improve partner nation and regional C5 capacity. The 2009 conference focused on "Enabling Regional Partnership through Multilateral Cooperation" followed by "Synchronizing Government, Commercial, and Military Network Communications Priorities" in 2010. The 2012 conference focuses on "Advancing Cyber Security Through Regional Cooperation". We lack a global Cyber cooperation strategy in which we can nest our plan. Therefore, our regional strategy seeks to engage communications leaders throughout the USCENTCOM AOR with a "whole of government" (State, Federal and Defense) approach concerning cyber-security and other topics of shared interest.

Partner Network: Although unilateral actions are at times necessary, sustained campaigns require a coalition-based operational framework. This framework requires a single "mission" network to be available in phase 0 enabling a single-force coalition fight. Operation UNIFIED PROTECTOR demonstrated that the requirement is not limited to the USCENTCOM theater, it extends to other Combatant Commands. A pre-existing coalition framework did not exist to enable a coalition beyond the context of a NATO coalition significantly challenging the initial integration of Jordanian and United Arab Emirate Air Forces. To this end, we support a USCENTCOM Partner Network, which promotes a regional information exchange environment for bilateral and multilateral communities of interest.

Reinvest Critical Capital Assets: We are proactive in our housekeeping and good stewards of the investments we make in capital assets. Over the past 10 years, USCENTCOM and its components procured 107 Deployable Ku-band Earth Terminals (DKETs), over 600 Very Small Aperture Terminals (VSATs) of various types and dozens of modular Technical Control Facilities (TCFs). Many of these have no programmed operation and maintenance funds for post-war sustainment. Good stewardship requires re-capitalization of these investments where a cost/benefit analysis proves re-use is prudent. Priorities for this effort are first within USCENTCOM, then to the other Combatant Commands, Agencies, Organizations and the Services Program Offices.

Additionally, USCENTCOM must work with the Services and within the existing processes to develop prepositioned C5 nodes capable of deployment within USCENTCOM, or perhaps globally, to support contingency operations. When additional equipment is available, we coordinate with the Joint Staff and other COCOMs to mitigate their un-resourced requirements. Expediency is paramount on this initiative to avoid equipment getting "lost" in the inertia of the numerous processes or become damaged through exposure to the elements.

Cyber Vigilance: Even with a robust regional partner network, the requirement for cross-domain solutions remains. The lack of interoperability between our networks forced several de-centralized solutions for cross-domain information sharing, which are both resource intensive and risky. USCENTCOM J6 is an advocate for the enterprise approach to Cross-Domain Solutions. The intent is to facilitate easier sharing of authorized information while preventing Cross Domain Violations and Negligent Discharges of Classified Information (NDCI).

As we create more classified networks (e.g., CENTRIXS-ISAF) and expand both their footprint and interconnection points via cross-domain solutions, spillages of information become more prevalent. To help mitigate the negative impact of spillages, service components provide robust training and awareness programs focusing on existing threats and operational vignettes. These programs must leave the user with an understanding of the potential impact to the warfighter due to either NDCI or Cross Domain Violation.

Governance: Successful transformation of the Command and its C5 Enterprise requires a strong governance framework to inform decision-making and ensure the Command effectively and efficiently leverages its C5 resources for both strategic and operational outcomes. The Command Chief Information Officer's (CIO) framework for governing the Command C5 Enterprise, depicted in Figure 1, is a holistic framework to address supporting and supported doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P).
(U) The Command C5 Enterprise governance framework provides key elements that ensure capabilities:

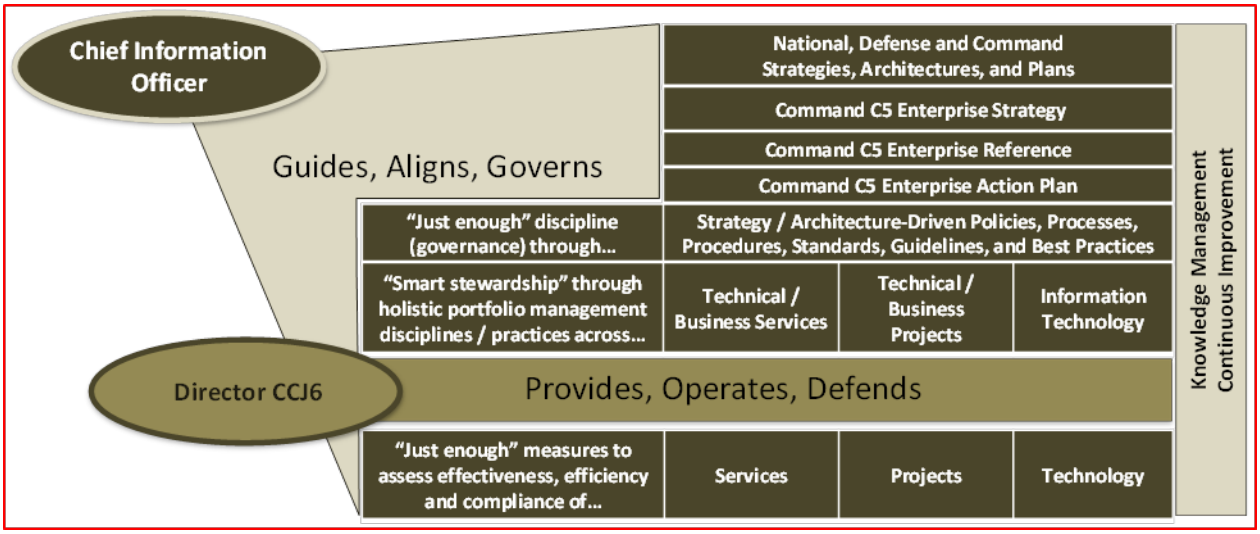


Figure 1: Command C5 Enterprise Governance Framework
- C5 Strategy guided by national, Defense and Command strategies, architectures and plans
- C5 Enterprise Reference aligned with national, Defense and Command architectural documents
- C5 Action Plan, or roadmap, to fulfill evolving/future requirements
- Disciplined governance through strategy/architecture-driven policies, processes, procedures, standards, guidelines, and best practices
- Holistic portfolio management disciplines across C5 technical and business services, projects, and assets/capabilities
- Measures to assess C5 effectiveness, efficiency, and compliance

Command C5 planning, led by the Chief Information Officer (CIO)/CCJ6 Director, ensures responsible application of C5 technology to Command priorities and emerging challenges at Command and theater levels. Command C5 planning ensures those who guide, align, govern, provide, operate and defend the C5 Enterprise maintain awareness of evolving challenges, requirements, and priorities.

As Operation ENDURING FREEDOM transforms during this period, USCENTCOM is refocusing on new capabilities that shore capability gaps noted in current operations and prepare for contingency operations. The USCENTCOM intends to deliver a Partner Network allowing full integration and compatibility with the Future Mission Network. The Partner Network conceptually enables information sharing tools with regional partners.

Future mission networks must facilitate rapid expeditionary expansion, and integrate into an enterprise environment enabling critical coalition and joint information exchange. Insufficient and unbalanced C5 infrastructure and a shortage of mobile command and control capabilities place our warfighters, along with coalition partners, in immediate danger and jeopardize mission accomplishment. USCENTCOM must continue closing capability gaps to enhance and evolve our C5 technologies -- meet mission needs, multiply force effectiveness, and operate in a dynamic theater.

Cyber organizational structure matures during this mid-term period. The future theater Cyber Forces re-organizes into a Joint Cyber entity. This organization provides support to the theater cyber forces as well as conducts direct coordination with USCYBERCOM and the Service Cyber forces. With a clear concept of operations, we overcome the complexities of split C2, one for global operations and one for theater support missions. The future model apportions forces and assets in each theater where the parent command retains the ability to direct these forces in the event of global priorities.

The objective model must balance the need for rapid global network response actions with the need for precise coordination, timing and tempo of theater operations. The objective model (Figure 9) clarifies C2. The Joint Task Force (JTF) Cyber elements work directly for the JTF commander; however, the cyber forces are imbedded within the Service Cyber elements and require a great deal of support from the joint cyber entity and the service headquarters for expertise and situational awareness. Despite fiscal constraints, in line with the 2012 DoD Priorities for the 21st Century, USCENTCOM must retain and build key advances in network warfare capabilities.

The Joint Staff Command, Control, Communications, and Computer Systems Directorate published the following goals in the Joint Net-Centric Operations (JNO) Campaign Plan:

Goal 1 – **Connect the Warfighter** - It is essential that seamless communications services be available to joint warfighters and mission partners under all conditions and at every echelon - especially at the “first tactical mile.”

Goal 2 – **Leverage the Power of Enterprise Services** - Provide the warfighter with common enterprise solutions to improve information sharing and combat effectiveness.

Goal 3 – **Secure the Network** - Provide the warfighter an assured information environment, protected and defended throughout the battlespace and across the entire network.

Goal 4 – **Accelerate Information Sharing** - Develop a strategy that supports cross-mission area and cross-domain information sharing throughout the battlespace.

Goal 5 – **Synchronize Delivery of Network Capabilities** – Strengthen joint warfighting by synchronizing delivery of capabilities and ensuring integration of capabilities across the entire Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel and Facilities (DOTMLPF).

Goal 6 – **Transform GIG Enterprise Management and Enhance Electromagnetic Spectrum Access** - Support Joint Network Operations (JNO) through improved GIG enterprise management, including electromagnetic spectrum management at all echelons.

USCENTCOM J6 Directorate (CCJ6)
The CCJ6 directorate is comprised of seven divisions: Cyber Security Division (CCJ6-C), Engineering Division (CCJ6-E), NetOps Division (CCJ6-O), Architecture and Programs Division (CCJ6-P), Resources and Analysis Division (CCJ6-R), C4 Systems Division (CCJ6-S), CDRUSCENTCOM established the Chief Information Officer (CIO) role and appointed the CCJ6 as the CIO.

Mission: CCJ6 will effectively and efficiently enable information sharing anytime and anywhere through a Joint and Combined C4 Network-Centric Environment that is flexible, redundant, reliable, secure, and protected.

Goals:

Goal 1: Align NetOps actions from the strategic to the tactical

Goal 2: Synchronize actions within the theater.

Goal 3: Issue clear and concise guidance to Components and Joint Task Forces.

Goal 4: Enable information sharing while ensuring information protection.

Goal 5: Continue to develop a results oriented team of professionals.

Goal 6: Capture AOR lessons learned to ensure we are correctly postured right for the next operation or contingency.

Goal 7: Improve CCJ6 business operations, postal services, and command records.

USCENTCOM CCJ6 Director/Chief Information Officer (CIO) Priorities: CCJ6 priorities support the goals established by the Joint Staff's "Joint Net-Centric Operations Campaign" and the USCENTCOM's "C5 Theater Strategy." The USCENTCOM CCJ6 Director/CIO created the following priorities to achieve the appropriate Network Centric Operational Environment (NCOE) in the USCENTCOM Area of Responsibility (AOR):

- **Central Command Commander:**
  - Commander/Deputy Commander Communications Support
  - Embassy Communications
  - Preparation to Support Numbered Plans
  - "Phase 0" Posture
  - Cyber Vigilance Campaign
- **Transformational:**
  - "C5 Enterprise Strategy" to " C5 Enterprise reference" to "C5 Enterprise Action Plan"
  - Warfighting Network "New Norm"
  - Central regional Communications Conference, 2012 (CRCC-12)
  - Structured information Management
- **Operational:**
  - Office of Defense Representative Pakistan
  - Afghan Transition
  - Future Planning
  - Combined Enterprise Regional Informational Exchange System – International Security Assistance Force Operational Assessment/Enduring Framework
- **Steady State:**
  - The "Human Dimension"
  - Network Operations
  - Disaster Recovery
  - Operating within Resource Restraints
  - Postal Operations Oversight (not a part of this contracting effort)

Other Information.

Headquarters Support: Headquarters Support represents our HQ C5 capabilities in and outside of the continental United States (CONUS), to include the Commander's aircraft. It includes programs, facilities, and assets such as the USCENTCOM Forward Headquarters (CFH), HQ, and Command Center C5 services and upgrades, Coalition Village C5 support, continuity of operations (COOP) capability, video teleconferencing (VTC) support, Command Information Management programs, and evolving USCENTCOM data automation.

USCENTCOM has a foundation that includes global communications capabilities and programs that address information and systems management, information operations (IO), information assurance (IA), and interoperability.

United States Central Command continues its full engagement in the war on terrorism and support of overseas contingency operations. USCENTCOM continues to evolve its C5

architecture into a robust, fully integrated and interoperable enterprise that is flexible enough to support the dynamic nature of operations anywhere in the USCENTCOM area of responsibility.

Sizing Information

C.5.2.1 C3 Systems Support

C.5.2.1.1 Management of HQ Systems Network Infrastructure

HQ USCENTCOM (Tampa)

- Operations
  - Approximately 617 Cisco routers/switches
  - Approximately 25 Cisco firewall/VPN devices
  - Equipment preventive maintenance inspections on approximately 30 switches, routers, modules, various vendor appliances, etc.
  - Approximately 150,000 IP addresses
  - Coordinate and ensure completion of 12 authorized outages a month
  - Approximately 1100 support calls a month
  - Approximately 50 daily system operations validation tests
  - Detailed diagrams for 12 disparate network infrastructures
  - Bench stock of approximately 100 switch/routers modules, transceivers', chassis', various vendor appliances, etc.
  - Approximately 50 separate operations files

- Scope of Equipment in operation
  - Cisco Routers: 185
  - Cisco Switches: 400
  - Cisco Firewall/VPN appliance (ASA): 20
  - Cisco Network Analysis Modules (NAM): 12
  - Riverbed WAN Accelerators: 5
  - DHCP Appliances: 10
  - Cisco Virtual Switches: 6

HQ USCENTCOM (CFH)

- Operations
  - 10 disparate network infrastructures
  - Approximately 150 Cisco routers/switches
  - Approximately 11 Cisco firewall/VPN devices
  - Equipment preventive maintenance inspections on approximately 15 switches, routers, modules, various vendor appliances, etc.

- Approximately 100,000 IP addresses
- 10 authorized outages a month, on average
- Approximately 200 support calls a month
- Approximately 20 daily system operations validation tests
- Bench stock of approximately 100 switch/routers modules, transceivers', chassis', various vendor appliances, etc.
- Approximately 30 separate operations files

C.5.2.1.2 Voice Services

- Operations
  - Approximately 13 Cisco Call managers
  - Approximately 6 Meeting Place Servers
  - Avaya CS-1000M telephone switch
  - Fault isolation of approximately 40 incidents a month
  - Approximately 20 change requests a month
  - 1 authorized outage a month, on average
  - Approximately 300 customer inquiries a month
  - Approximately 10 separate operations files
  - Equipment preventive maintenance inspections on approximately 12 items
  - 4 disparate VOIP network infrastructures
  - Bench stock of approximately 20 items that include but is not limited to DSN phones, STEs, VOSIP phones, jumper wire

- Scope of equipment in operation
  - Cisco 7835 Call manager: 10
  - Cisco Meeting Place Web Server: 1
  - Cisco Meeting Place Audio Server: 1
  - Cisco 7975 Phones: 1417
  - Cisco 7971 Phones: 136
  - Cisco 7970 Phones: 75
  - Cisco 7965 Phones: 264
  - Cisco 7961 Phones: 298
  - Cisco 7960 Phones: 234
  - Cisco 7941 Phones: 179
  - Cisco 7940 Phones: 32
  - Cisco 7912 Phones: 13
  - Cisco 7936 Phones: 5
  - Cisco 7937 Phone: 1
  - Avaya CS-1000M switch: 1
  - Analog TDM Phones: 1547
  - Digital TDM Phones: 1698
  - ISDN: 12

C.5.2.1.3 Patch and Test Facility Support

- Operations

- Fault isolation of approximately 90 circuits a month
- 16 authorized outages a month, on average
- 30 circuit validations a month
- Approximately 250 customer inquiries a month
- Approximately 85 encryption devices loaded a month
- Responsible officer duties (SVRO) accounting for approximately 10 FORTEZZA Cards
- Approximately 30 separate operations files
- Equipment preventive maintenance inspections on approximately 60 items
- Bench stock of approximately 40 items
- 30 pieces of test equipment
- 50 individual tools

- Scope of Equipment in operation
  - Channel Service Units and ancillary equipment: 181
  - Integrated Services Digital Network equipment: 33
  - Digital Patch Panels: 54
  - Pairgain Digital Subscriber Line MODEMS: 30
  - Encryption devices and associated ancillary equipment: 244
  - Promina nodes and ancillary equipment: 2
  - SONET nodes and ancillary equipment: 8
  - Fiber optic MODEMs/fiber optic transceivers: 219
  - Test equipment: 124

C.5.2.1.4 Cable Plant Support

HQ USCENTCOM (Tampa)

- Operations
  - 52 Telecommunication Rooms (TRs)
  - Approximately 10 authorized outages a month
  - Approximately 400 support calls/tickets a month
  - Approximately 10 quarterly Preventive Maintenance Inspections (PMIs) per quarter
  - Detailed documentation for 12 disparate cable infrastructures
  - Bench stock of approximately 3000 items such as various types of fiber patch cables, transceivers, connectors, test equipment, etc.
  - Approximately 20 separate operations files

- Scope of Equipment in operation
  - Copper cable test kits: 6
  - Fiber Optic cable test kits: 6
  - Fiber Optic Transceivers (FOTs): 100
  - Copper/Fiber Patch Cords:3000

HQ USCENTCOM (CFH)

- Operations
  - 2 routine site visits per year to inspect cable management
  - 16 Telecommunication Rooms (TRs)
  - 1 Preventive Maintenance Inspections (PMIs), per quarter, at USCENTCOM Forward Headquarters (CFH) and its remote managed site in Bahrain.
  - Detailed documentation for 8 disparate cable infrastructures
  - Bench stock of approximately 1000 items such as various types of fiber patch cables, transceivers, connectors, test equipment, etc.
  - Approximately 10 separate operations files

- Scope of Equipment in operation
  - Copper cable test kits: 2
  - Fiber Optic cable test kits: 2
  - Fiber Optic Transceivers (FOTs): 100
  - Copper/Fiber Patch Cords: 1000

C.5.2.2 Enterprise Network Services Support

C.5.2.2.1 Communications Center

HQ USCENTCOM (Tampa)

- Operations
  - Receive over 53,000 DMS messages per month, of which approximately 2,000 messages are high precedence and / or special handling that require special processing
  - Management of 150 communications circuits, of which approximately 40 are re-keyed per month
  - COMSEC account with approximately 80 line items
  - 631 user and organizational accounts

- Scope of Equipment in operation
  - 2 AMHS servers over multiple domains
  - 2 Directory Service Agent Servers
  - 2 Certificate Authority Workstations
  - 6 Administrative Directory User Agents
  - 1 AMHS Data Server (Symantec Backup Exec)
  - 6 Simple Key Loader (SKL)
  - 2 Data Transfer Device
  - 150+ circuit updates
  - 1 Top Secret Collateral AMHS Client
  - 1 Top Secret JWICS M3 Client

HQ USCENTCOM (CFH)

- Scope of Equipment in operation
  - 2 AMHS servers over multiple domains with 600 accounts

- 2 Directory Service Agent Servers
- 2 Certificate Authority Workstations
- 4 Administrative Directory User Agents
- 2 Data Transfer Device
- 1 Top Secret Collateral AMHS Client

C.5.2.2.2 GCCS Support

HQ USCENTCOM (Tampa)

- Operations
  - 230 IT systems
  - 4 authorized outages a month, on average
  - 12 daily system operations validation tests
  - Detailed diagrams for 6 disparate data architectures
  - Bench stock of approximately 150 items to include hard drives, memory, KVM devices and assorted peripherals
- Scope of Equipment in operation
  - Servers
    - 23 physical and 37 virtual UNIX servers on SIPRNet
    - 1 physical and 14 virtual Windows servers on SIPRNet
    - 6 physical and 6 virtual UNIX servers on CENTRIXS
    - 6 physical Windows servers on CENTRIXS
    - 2 Multi-Domain Guards
    - 4 VMWare ESX servers on SIPRNet
  - Workstations (Tampa)
    - 81 Windows XP based workstations on SIPRNet and CENTRIXS
    - 50 Virtual workstations on SIPRNet

HQ USCENTCOM (CFH)

- Operations
  - 90 IT systems
  - 4 authorized outages a month, on average
  - Approximately 50 daily system operations validation tests
  - Bench stock of approximately 80 items to include hard drives, memory, KVM devices and assorted peripherals
  - 7 disparate data architectures
- Scope of Equipment in operation
  - Servers (CFH)
    - 15 physical and 30 virtual UNIX servers on SIPR
    - 7 virtual Windows servers on SIPR
    - 5 physical and 5 virtual UNIX servers on CENTRIXS
    - 5 physical Windows servers on CENTRIXS
    - 2 Multi-Domain Guard
  - Workstations (CFH)

- 14 physical and 7 virtual Windows XP based workstations on SIPRNet and CENTRIXS

C.5.2.2.3 End-User Information Technology (IT) System Support

- Approximately 1,500 printers
- Approximately 5000 Thin Clients, 4700 Workstations and 200 Laptops (not users). OS is Microsoft Windows 7
- Bench stock of approximately 250 items to include hard drives, memory, KVM devices and assorted peripherals
- Supprt, on average, about 1 – 2 local conferences per month.

C.5.2.2.4 Server Operations and Maintenance Support

- Approximately 800 Servers (55/45% physical/virtual)
  - Core and server farm operating in virtual server environment using VMware software
  - Operating environment is Microsoft's Active Directory, Windows 2008 server, Unix (Sun Solaris), Linux and Exchange 2010 utilizing Enterprise vault
- Approximately 1,500 printers
- Approximately 5000 Thin Clients, 4700 Workstations and 200 Laptops (not users)
- Approximately 8200 user accounts
- Manages 1.2PB of storage on EMC DMX 4 CELERRA, Clarion, VNX, Recover Point, Data Domain and AVAMAR as the tapeless backup system.

Coalition networks

Four CENTRIXS Coalition; each network extends to various sites throughout the USCENTCOM AOR and contains an enterprise at HQ USCENTCOM. Each enterprise contains servers which provide the following: Domain Controllers, Domain Name Services, electronic mail, anti-virus, chat, global address list synchronization, internet locator service, and voice over internet protocol call management. A storage area network is used to back-up the data.

CENTRIXS Bilateral Networks; USCENTCOM maintains bilateral networks with other countries to support exchange of intelligence and operational information. In comparison to Coalition networks, these are significantly smaller. Each network contains an enterprise at the HQ. The enterprise consists of servers providing the following: Domain Controllers, Domain Name Services, electronic mail, anti-virus, web, and internet locator service. A storage area network is used to back-up the data. Additionally, similar servers exist in the other country on selected networks. Size of each bilateral network is approximately 200 users.

C.5.2.2.5 Wireless Communications

- Approximately 650 Cell Phones/BlackBerry Devices
- Approximately 300 Pagers

- Approximately 30 iPad/iPhones
- Approximately 30 Samsung Tab 10.1/Samsung Galaxy SIIs
- Approximately 80 Secure Mobile Environment Personal Electronic Devices (SME PEDs)
- Approximately 10 Secure deployable communication kits
- Approximately 60 WIFI and Air Cards
- 2 Desktop systems
    - Running Blackberry Desktop software
    - iTunes for IOS devices
    - PC Updater, Hyper Terminal, and MS Sync for certificates for SME PED
    - Dialup utility for pager system
- 2 Desktop systems
    - Running Blackberry server tools (Blackberries)
    - Running Good Server tools (Android, Apple)
    - Running SENSA Server tools (SME PED)
- 80 VIP users supported

C.5.2.3 Operations Support

C.5.2.6 HQ User Training

The following courses are expected to be taught on a reoccurring basis based of the need USCENTCOM and able to teach up to 20 students at the same time. Classes will be mixed.

- Cisco Certified Entry Level Technician Exam (CCENT)
- Cisco Certified Network Associate Exam (CCNA)
- Microsoft Configuring & Troubleshooting Windows Server 2008 Active Directory Domain Services (WSAD)
- Microsoft Configuring & Troubleshooting Windows Server 2008 Network Infrastructure (WSNI)
- Deploying Windows Server 2008 (DWSV)
- Configuring & Administering Windows 7 ((CAW7)
- Designing a Windows Server 2008 Active Directory (DWAD)
- Implementing & Managing Windows Server 2008 Hyper-V (IMWS)
- Share Point Site Designer
- Remedy Analyst
- ITSM 4 Hour Introduction
- CompTIA Network+
- CompTIA Security+
- CompTIA A+ Certification
- ITIL v3 Foundations
- Certified Information Systems Security Professional (CISSP)
- Project Management Professional (PMP)®
- CCNP- Route, Switch
- Microsoft Office Applications Training
- Information Assurance Training

C.5.2.3.1 Visual Information Systems

130 Video Teleconferencing / Briefing Suites
6 VTC Hubs in HQ, 2 in CFH – all Cisco equipment

Total Supporting Equipment

	GO/FO	OPS CNTR	Conf Rm
570 1st FL	7	0	7
570 2nd FL	1	4	2
570 3rd FL	4	0	14
570 4th FL	17	4	10
CV3	1	0	3
CTF	0	0	3
HQCOM	0	0	1
CFH	7	4	31
565	0	0	8
CRC	0	0	2
Total	37	12	81
		Room Total	**130**

Average 63 Audio-Visual events & 410 VTC events per month in HQ, 50 combined in CFH.
MCU bridge (Cisco Codian or similar)
CODECS (Cisco / Tandberg MXP Series, C Series, or similar)
ISDN Modems (Adtran Atlas 890 or similar)
Encryption devices (KIV-7s or similar)
Crestron Controller systems (Crestron or similar)
Desk Top VTC Units (Cisco / TANDBERG 1700s or similar) 227 each
TV's 330 each
Video Display Walls (Planar/ Barco) 12 each (6 in HQ, 6 in CFH)

Networks/media VTCs traverse

- ISDN 8 each
- DVS
- IP
- Dedicated Circuit 1 Each

C.5.2.4 Customer Support Operations

HQ USCENTCOM (Tampa)

- Operations
  - Approximately 4,500 phone calls per month to the Service Desk.

- Approximately 260 change requests opened per month via phone, email or web interface.
- Approximately 4,000 tickets opened per month via phone, e-mail, web interface or walk-in.
    1. Approximately 3,000 tickets are generated from phone calls.
    2. Approximately 400 tickets are opened via walk-in.
    3. Approximately 800 tickets are opened via the web.
    4. Less than 40 tickets are opened via email.

- Scope of Equipment in operation
    - Automated Call Distribution (ACD)
    - Common Access Card (CAC) Pin Reset

HQ USCENTCOM (CFH)

- Operations
    - Approximately 300 tickets opened per month via phone, e-mail or web interface
    - Approximately 600 phone calls per month to the Service Desk
    - Approximately 25 change requests opened per month via phone, email or web interface

- Scope of Equipment in operation
    - Common Access Card (CAC) Pin Reset

C.5.2.5 Commander's Communications Support

- Approximately 5 travel pack-outs per month – up to 2 overseas and 3 stateside
    1. Overseas Packout - Up to 40 communications equipment cases, etc.
    2. Stateside Packout - Up to 20 communications equipment cases, etc.
- 120 laptops
- 20 remote reach back kits
- Up to three home stations – Two located at HQ USCENTCOM in Tampa and one located at CFH, Qatar

C.5.3 Task Area 3 – Theater Network Operations (NetOps) Support

Promina Theatre Network Operations (Tampa)

- Approximately 200 tickets per month
- Approximately 2000 phone calls per month to the Theatre Network Operations (TNC) floor. (not all result in a ticket)
- 65 remote management nodes (Promina Domain 30 Network)
- 1 seed node collecting traps from Domain 30 Promina network
- 1 physical server running network management system (NetMS)
- Operating environment is the Windows server 2008/R2
- Approximately 6 Workstations/Laptops with latest approved Microsoft OS

Promina Qatar (COOP Site)

- 1 seed node collecting traps from Domain 30 Promina network
- 1 physical server running network management system (NetMS)
- Operating environment is the Windows server 2008/R2
- Approximately 6 Workstations/Laptops with latest approved Microsoft OS.

Information Technology Service and System Management

- 80 Internet Gateway Exchange (IGX) voice switches supporting the Tier 1 and Tier 2 level theater voice network.
- 10 SMU voice switches supporting the Tier 1 and Tier 2 level theater voice networks which supports over 50,000 subscribers.
- 5 Defense Red Switch Network (DRSN) switches supporting over 350 customers supporting NCA level (JCS, NSA, OSD) C2 secure communications.
- 60 tactical voice switches supporting the Tier 1 and Tier 2 level theater voice networks which supports over 60,000 subscribers.
- 7 Sl-100 DSN voice switches supporting the Tier 0 and Tier 1 level theater voice networks which supports over 80,000 subscribers.
- Over 100 Tier 1 IP switches and routers for all components within the USCENTCOM AOR.
- Over 200 Tier 1 IP switches for all components.
- Over 1000 firewalls for all components.
- Over 100 Intrusion Detection Systems (IDS) for the SIPRNet and NIPRNet networks within the USCENTCOM AOR.
- VOIP network supporting over 400 customers
- 10 CONOPS annually.
- 60 video type systems (VTC, ISDN, JWICS, Global Broadcast Service (GBS)) within the USCENTCOM.
- Coordination with five to seven different NetOps Centers on a daily basis.
- 15 JCS recurring RFI/Taskers in support of GO/FO level inquires.
- IAVA reporting from 5 components and 3 CJTFs which tracks over 20,000 AIS systems.
- 10 weekly Status reports from each component.
- Over 360 CAP packages from each of the components and USCENTCOM HQ. (Process 8-10 daily).
- Network Scans: Analyze, collect, audit data from weekly network scans from over 700 IP which produce over 600 finding. Some findings require fault management.
- Quarterly vulnerability scans: Analyze, collect and audit data done from vulnerability scans by conducted by subordinate organizations and components. Each scan averages about 800 findings.
- 2100 average monthly incidents track via a database. Trend analysis and fault management required.
- Accreditation package Circuits: Verify, track, re-accredited 150 packets for (NIPR/SIPR) circuits.

- Accreditation package Systems: Verify, track, re-accredited 140 packets for (NIPR/SIPR) systems.
- Circuit Actions (PROCESS REQUESTS/DATABASE MANAGEMENT) Management of all circuit requirements requests for services. This includes direct coordination with Component and Joint Task Force Commanders and DISA organization ensure smooth, seamless processing of all requirements; 9,000 annually.
- Commercials Satellite Surveys, 200 annually.
- Management of all Satellite / Gateway Access Request and Requests for services. This includes direct coordination with Component and Joint Task Force Commanders and DISA organization ensure smooth, seamless processing of all requirements; 3000 annually.
- Aaverage of 25 DMS messages a month.
- Average of 3-4 RFI/Taskers or fault management problems a day.

C.5.4 Task Area 4 – Engineering Support

Relevant Tools

Analyst NoteBook	Wireshark	Hyperion Intelligence Client
ArcSight Event Security Manager	Clarious IPC	IP Communicator
Bluecoat Reporter	Prognosis	Managed Server
CA Gigastor	Route Explorer	Security Desktop Agent
CA Net Voyant	Traffic Explorer	Security Server Agent
CA Network Performance Center	ADIMSS	Silvex
CA Reporter Analyzer	CCSD Database	SMC-II
CA Spectrum	DDOE (DISA Direct Order Entry)	BlackBerry Server
Cisco Network Compliance Manager	ESRI ArcGIS	SharePoint
COMPLAN	HOTR	Solaris
DII Guard	INMS	VOSIP/STE/DRSN/DSN
Discover Attender	IP Sonar	ArcSight Content Management
eEye Retina	JCD (Joint Capabilities Document)	ArcSight IPCCM
HBSS	MRTG (Multi Router Traffic Grapher)	ArcSight Network Defense
ITSM	NCCM (Configuration Management)	CA eHealth
Microsoft App-V	Net MS	CA eTrust Auditor
OPNET	NetHealth (CA eHealth Suite)	CA ITechnology Igateway
Putty	Ticket Management System (TMS)/RMS	HBSS ePO Asset Rollup

Radius TACACS	US-CERT (G First)	HyperIP for VMWare
Remedy 7.6.04	WWOLS (Worldwide Online System)	SMC (Service Management Console)
System Center Configuration Manager	ALPS	WSUS
System Center Operations Manager	Content Security and Control	Digital Fountain
Super Agent	Dande	Enterprise Capability Management
TRIM	EIQ Network Enterprise Analyzer	Netcool/ISM Protocol Managing Server

C.5.4.1 Project Management

- Approximately 95 IT projects at any one time.

C.5.4.2 Engineering Support

C.5.4.2.2 Engineering Design Analysis

- 10 VoIP Gatekeeper Clusters. Manage configuration, design, fault management and support infrastructure of over 5 Local Session Controllers (LSCs).
- Over 150 Tier 1 routers for all components within the USCENTCOM AOR.
- Over 150 Tier 1 switches for all components within the USCENTCOM AOR.
- 15 CONOPS annually.
- Over 60 video type systems (VTC, ISDN, JWICS, GBS) within the USCENTCOM.
- 7 bi-lateral agreements between host nation and US Military.
- Coordination with 5 war fighting components and 3 CJTFs in support of future and current planning. Help write and maintain Annex Ks and OPLANs for each of them.
- 10 Requests for Forces (RFF)/DEPORDS per week, 300 per year.
- 15 JCS recurring RFI/Taskers in support of GO/FO level inquires.
- 10 weekly Status report from each component.
- Weekly network scans from over 700 IP which produce over 600 finding.
- 2100 average monthly incidents track via a database
- SHF (PROCESS REQUESTS/DATABASE MANAGEMENT)
  Satellite and Gateway Access Requests; 500 annually.
- EHF (PROCESS REQUESTS/DATABASE MANAGEMENT)
  100 Satellite Access Requests annually.
- KU (PROCESS REQUESTS/DATABASE MANAGEMENT)
  Commercials Satellite Surveys, 200 annually.
- SAR/GAR/RFS
- Management of all Satellite / Gateway Access Request and Requests for services. This includes direct coordination with Component and Joint Task Force Commanders and DISA organization ensure smooth, seamless processing of all requirements; 1500 annually. Maintain database and web page.

- Gaps identification in Policies and CONOPS on a bi-annually basis.
- Average of 3-4 RFI/Taskers a day.
- Gap identification in Annex K and 5 OPLANS on a bi-annual basis.
- Engineering of ArcSight Security Information Event Management (ESM)
- Engineering of Host Base Security Systems (HBSS) to integrate multiple information assurance, network defense, and NetOps capabilities from compliance monitoring to automated incident reporting

C.5.4.2.4 Configuration and Enterprise License Management

- Approximately 19,000 configuration items categories in the Configuration Management Database
- Approximately 1,100 tickets (change request/work orders) submitted monthly

C.5.4.3 Test, Analysis and Integration Lab Support

- Average number of task received per month is approx. 75 task
- Average number of load set releases per month is 3 on NIPR and SIPR
- Average number of IAVAs tested per month is approx. 24 test
- VDI recomposes are conducted monthly on average
- Support to 4 different networks: NIPR/SIPR/2 Coalition Networks

C.5.4.4 Software Engineering Support

- Approximately 45 SQL servers (stand alone or clustered) on multiple networks supporting over 100 databases instances, approximately 775 databases and approximately 300+ web applications.
- Approximately 14 physical and virtual web servers on multiple networks.
- Manages approximately 35 major projects and 300+ service desk requirements on a monthly basis.

C.5.5 Task Area 5 – Cyber Security

C.5.5.1 Headquarters Network Defense

- Average 300+ network or system scans for vulnerability/risk assessments per month
- 80 Information Assurance Vulnerability Alerts/Bulletins;
- Average of 215 security reports and initiate an average of 20 incidents to investigate per month
- Average of 50 security events; working across Directorate for coordination and collaboration per month
- Average 95 tickets of customer inquiries, issues or requests per month
- Average of 240 Requests for Information (RFI) per month
- 130 network defense tools/systems throughout the Enterprise
- Average 10 external office or agency inquiries and investigations per month
- Average of 10 Joint Staff/Command-initiated Taskers; prepare responses for leadership per month

- Large quantities (terabytes) of data for anomalous activity/behavior; provide leadership with briefs/assessments/mitigations

C.5.5.2 Theater Cyber Initiatives

- 140 Requests for Information (RFI) from Components per month
- 4-6 Orders (CENTCOM Command Tasking Orders, Fragmentary Orders, etc.) per month
- Average of 12 Joint Staff/Command-initiated Taskers.
- Average of 24 projects for the Command and theater initiatives per month
- Average of 15 briefings to support senior leader understanding, engagements or project status/updates per month

C.5.5.3 Cyber Certification and Accreditation

- Approximately 8 System Security reviews for the Headquarters Enterprise per month
- Approximately 8 assessments in support of theater systems/applications through the CCR 25-200 submissions for the theater Components per month
- Average of 12 Certification & Accreditation projects per month
- Approximately 15 unique scans to assess system compliance per month
- Approximately 7 packages for Designated Approving Authority (DAA) signature per month
- Average of 15 Joint Staff/Command-initiated taskers; prepare responses for leadership per month

C.5.7 Task Area 7 – Resource Management Support

C.5.7.1 Records Management

- Migrate on average 200,000 records per month into TRIM

C.5.7.2 Asset Management

- Supporting Bahrain, Qatar and Kuwait
- Total numbers of assets are as follows: Qatar 16,000/Bahrain 3,500/Kuwait 1,250.

Attachment Q
Monthly Status Report

MONTHLY STATUS REPORT for (Month and year)

Contractor	
Contract Number	
Task Order Number	
FAS Project No.	
Contractor's Project Manager Name / Phone Number	
Date of Award	
Period of Performance	
Task Order Award Amount	

Financial

- Total billed hours for this period and to date
- Total Costs plus Estimated Award Fee (if applicable) for this period and to date
- Items purchased for the Government (CLINs xxx and xxx)
- Travel costs

Program Support

- Staffing Losses and Gains and related impacts
- Proposed Staff Training
- Significant concerns
- Quality Assurance Report
- Quality Improvement Efforts
- Government actions required
- Trips taken, conferences attended, etc.
- Schedule (Shows major tasks, milestones, and deliverables; planned and actual start and completion dates for each)

Prepared by: (Signature) _____ (date) _____
(Name)
Project Manager

Attachment R
Non-Key Personnel Knowledge and Skills

The following are the desired non-key personnel knowledge and skills by task.

Task	Desired Qualifications
C.5.2.1.1 HQ Systems Infrastructure	Shall be a CISCO Certified Network Associate/Professional (CCNA/CCNP). Knowledge of network analysis tools CISCO Network Configuration Manager, CISCO Adaptive Security Device Manager, Net Flow, Simple Network Management Protocol, etc.). WAN troubleshooting / problem determination skills (ISDN, ATM, SONET, etc.). LAN troubleshooting /problem determination skills (Ethernet, HSRP, EIGRP, BGP, etc.). Knowledge of CISCO firewall/VPN equipment, (Adaptive Security Appliance, etc.), NEXUS Data Center Architecture, CISCO ASR, and VSS. Knowledge of IP services (IP, Multicast, SNMP, etc).
C.5.2.1.2 Voice Services	Experience with operational and maintenance of voice services in a diverse environment including, but not limited to, Voice-over IP, Private Branch Exchange (PBX), ISDN, inside cable plant etc. CISCO Call Manager experience. Knowledge of voice analysis tools such as NETIQ. Demonstrated ability to configure, install and troubleshoot secure voice devices including but not limited to STEs, OMNIs, and VIPERs. Knowledge of VOIP quality services. Working knowledge of voice conferencing services (Bridges, Meeting Place, etc.). Ability to install/configure and troubleshoot ISDN services.
C.5.2.1.3 Patch and Test Facility (PTF)	Experience working in a DoD technical control facility or equivalent facility that terminates and operates/maintains telecommunications data circuits over the Defense Information System Network and commercial vendors and ability to troubleshoot ATM, SONET, and Promina systems. Demonstrate ability to operate data and fiber optic test equipment. Limited experience with radio frequency systems. Working knowledge of voice and video systems. Knowledge on basic telecommunication system theory and able to design long-haul systems traversing various interconnect technologies (cable, fiber, satellite, etc.). Thoroughly familiar with data interfaces used in terminating

	circuits on telecommunications systems. Ability to interpret telecommunications service orders and execute activation of circuits and systems.
C.5.2.1.4 Cable Plant Support	Experience maintaining operational cable infrastructures in a high paced diverse environment Knowledgeable of NECA/ BICSI 568 standards. Experience operating and maintaining cable plant infrastructures. Knowledge of cable infrastructure troubleshooting and analysis tools (Cat 5E and Cat6 copper testing kits, fiber optic test kits, dB loss testers, etc.). Knowledge of and the ability to perform various fiber optic splicing techniques. Knowledge of and the ability to perform various twisted-pair copper cabling termination techniques. Knowledge of various different fiber optic and twisted-pair copper cable specifications (Multi-mode, Single-Mode, 9/50/62.5um, Cat5e, Cat6, ST/SC/MTRJ/LC/RJ-45 connectors, etc.).
C.5.2.2.1 Communications Center	Extensive Systems Administration experience in a C2 system engineering and administration environment. Extensive experience with DMS C2 systems integration in a DoD environment. Experience with ADP acquisition planning for major Headquarters or regional site. Experience with major platform migrations to upgrade legacy systems. Remote systems and database management. Specialized in Joint Telecommunication Center operations at COCOM level. Certified or knowledgeable in COMSEC and CA Workstation. Extensive knowledge and training in Automatic Digital Information Network (AUTODIN_, DMS, and AMHS administrations. Possesses proficiency to perform CRO responsibilities, CA Workstation operations, and system operations tasks on a variety of cryptographic equipment.
C.5.2.2.2 GCCS Support	IAW DoD 8750, positions require incumbents to maintain industry recognized certification as Information Assurance Technical Level 3 (IAT 3). Skills associated with installation, maintenance and basic operations of GCCS servers and the Command and Control Personal Computer (C2PC) with emphasis on communications configuration, track data flow and synchronization of the COP. Operational experience working with the GCCS or any of its

	service variants (GCCS-M, GCCS-A, GCCS-AF, IAS/IOS (Internet Authentication System / Internetwork Operating System) , and/or Theater Battle Management Core System (TBMCS)) Extensive experience with installation administration and maintenance of Solaris 10, Windows 2003, XP clients and servers. UNIX Sybase database administration experience. Microsoft Certified Systems Administrator Certification. Technical Certification in Systems Administration for the Solaris 10 OS. On-the-job experience with the administration of GCCS-J or service-specific systems.
C.5.2.2.3 End-User Information Technology (IT) System Support	A+ Certification Security+ and Network+ Certifications, Dell Server 7.0 MCP (Windows XP workstation), Microsoft Certified Information Technology Professional (MCITP), CCNA, Nortel Network (Fiber Optic and Copper), ClearCube Blade certifications. On the job experience with hardware and software configuration management. IAW DoD 8570, positions require personnel to maintain industry recognized certification as Information Assurance Technical Level 2 (IAT 2).
C.5.2.2.4 Server Operations and Maintenance	IAW DoD 8570, positions require personnel to maintain industry recognized certification as Information Assurance Technical Level 2 (IAT 2). Microsoft Certified Systems Administrator (MCSA), Microsoft Certified Solutions Expert (MCSE), MCITP Certifications Extensive experience with administration, operation and maintenance of VMWare View, VMWare ESXi, Windows Server 2008, HBSS, MS SCCM, MS SCOM, MS Exchange 2010 and MS Active Directory.
C.5.2.4 Customer Support Operations	Shall have A+, N+, or Security + certification per DoD8570. Have experience with troubleshooting MS Windows 7 operating systems, Active Directory and MS Office products. Basic familiarity of network account concepts including creation, maintenance, and deletion. Basic understanding of ITIL foundation concepts relating to incident management principles. Experience adequate to provide Tier 1 support in the following areas: MS Office 2010, Win 7 Operating Systems,

	and Remedy Help Desk systems. HDI Service Desk training.
C.5.2.5 Commander Communications Support	Shall be CISCO CCNA. Shall have at least three years of experience managing operational networks in a high-paced, diverse environment. WAN troubleshooting/problem determination skills (ISDN, SONET, etc.). LAN troubleshooting/problem determination skills (Ethernet, HSRP, EIGRP, BGP, etc.). Knowledge of CISCO firewall/VPN equipment (Adaptive Security Appliance, etc.). Knowledge of IP services (IP, Multicast, QOS, SNMP, etc.). Familiarity with Joint Service operations.
C.5.2.6 HQ User Training	Training manager experience (developing training plans, public speaking, etc.). A+ and Network+ Certifications, Microsoft Office User Specialist (MOUS) (MS Word), MS Office experience, ITSM Foundations and PMP certifications,
C.5.3.3 Information Assurance - CND	IAW DoD 8750, position requires Contractor to maintain industry recognized certification as Information Assurance Manager Level 2 (IAM 2). IAW DoD 8750, position requires Contractor to maintain industry recognized certification as Information Assurance Technical Level 1 (IAT 1). Position requires Contractor to maintain Information Technology Infrastructure Library Version 3 (ITILv3) or later version certification.
C.5.4.1 Project Manager	Extensive experience managing IT projects throughout the project life cycle to include, but not limited to, initiating, planning, project execution, project monitor and controlling, and project closure. • Substantial experience with PMBoK Methodology • PMP Certification desired • ITIL Certification desired
C.5.4.2.2 Engineering Design Analysis	Have substantial familiarity with: • GIAP database • SNAP database • (PPSM • DoD Information Technology Portfolio Repository • DoD Information Technology SIPRNet Registry • eMASS • FISMA Local databases, sites, and systems.
C.5.4.2.5	ITSM Configuration Management II Courses I – VI, Remedy

Configuration and Enterprise License Manager	Asset, knowledge of portfolio management, Remedy Desktop and Server Management, Remedy Service Desk. Prior experience with contract/license management.
C.5.4.2.7 Change Manager	IT Service Management (ITSM/ITIL) certification, BMC Remedy experience, and ITIL Service Transition certification.
C.5.4.3 Integration Lab	All lab engineers should have substantial experience and possess any of the following minimal certifications: • Microsoft Certified Systems Engineer (MCSE) • MCSA • Computer Associates Certificate At least one engineer must be CISSP certified and/or be a GIAC Certified Windows Security Administrator (GCWN) OR GIAC Certified Enterprise Defender (GCED). At least one engineer must possess extensive experience with mobile device technology to include, but limited to, 3G/4G, Wifi / WiMax Technologies, Application Development, and mobile platforms (such as iOS, Android, etc.). • At least one engineer must possess extensive experiences with virtual environment setup and management.
C.5.4.4 Software Engineering Support	Extensive experience with Microsoft Office SharePoint Server (MOSS) portal to include building web parts. Understand active directory structure and the use of organizational units. Knowledgeable in managing virtual environments. Knowledgeable of MS Team Foundation Server software.
C.5.6.1.1 Program Planning and Development Support	50% or more of the proposed staff within this task should be PMP certified.
C.5.6.3 Architectures Support	50% or more of the proposed staff within this task should be DoDAF trained.

mod 18 funding table.xlsx